February 28, 2002

The Board of Commissioners of Public Utilities
Prince Charles Building
120 Torbay Road
St. John's, Newfoundland

ATTENTION: Ms. Cheryl Blundon
Director of Corporate Services and
Board Secretary

Dear Ms. Blundon:

Re: Hydro General Rate Application –
Undertaking re Information Technology –
Technical Architecture Strategy Report

During the recent Rate Hearing an undertaking was provided that Hydro would file a copy of the Information Technology – Technical Architecture Strategy Report when it was completed. This undertaking was provided by Mr. Budgell on November 5th, 2001.

This report has recently been finalized and seventeen (17) copies of the Report are enclosed with this letter as required by Hydro's undertaking of November 5th, 2001.

The IT – Technical Architecture Strategy Report summarizes Hydro's current business and technology landscape and future directions. It outlines the long term technical design and short term recommendations to achieve a reliable, secure and effective networking and processing architecture and provides a framework for an infrastructure to provide adequate performance for the next two to five years with a longer term vision of ten years. The recommendations in the Report are intended to assist in Hydro's development and implementation of a core technology program.

The filing of this Report was the last outstanding issue from the Rate Hearing.

Yours truly,

Maureen P. Greene
Vice-President Human Resources, General
Counsel and Corporate Secretary

MPG/mgw
Encls.

c.c. Gillian Butler, Q.C. and Peter Alteen
Counsel to Newfoundland Power Inc.
55 Kenmount Road
P.O. Box 8910
St. John's, Newfoundland
A1B 3P6

Janet M. Henley Andrews
Stewart McKelvey Stirling Scales
Cabot Place, 100 New Gower St.
P.O. Box 5038
St. John's, Newfoundland
A1C 5V3

and

Joseph S. Hutchings
Poole Althouse
P.O. Box 812, 49-51 Park Street
A2H 6H7

Dennis Browne, Q.C.
Consumer Advocate
c/o Browne Fitzgerald Morgan & Avis
P.O. Box 23135
Terrace on the Square, Level II
St. John's, Newfoundland
A1B 4J9

Mr. Edward M. Hearn, Q.C.
Miller & Hearn
450 Avalon Drive
P.O. Box 129
Labrador City, Newfoundland
A2V 2K3

Mr. Dennis Peck
Director of Economic Development
Town of Happy Valley-Goose Bay
P.O. Box 40, Station B
Happy Valley-Goose Bay
Labrador, Newfoundland
AOP 1EO

Aliant

IT TECHNICAL ARCHITECTURE STRATEGY REPORT

HYDRO

THE POWER OF COMMITMENT

February 18, 2002

xwave

AN ALIANT COMPANY

NEWTEL

an Aliant company

Table of Contents

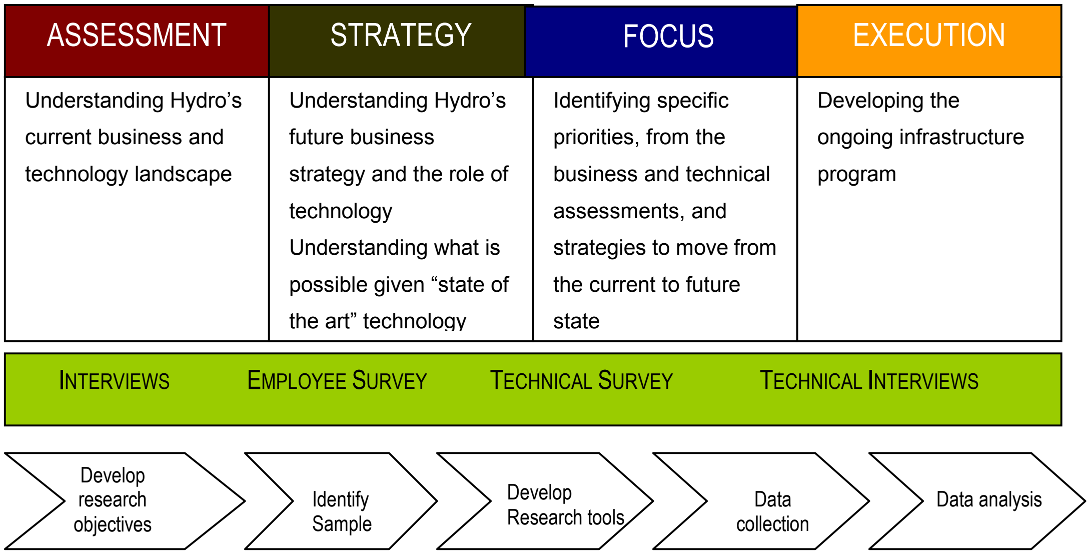
List of Figures:

1.0 Executive Summary

Background

The Newfoundland and Labrador Hydro (Hydro) Information Technology Technical Architecture Strategy Project reviewed Hydro's current business and technology landscape, identified the Corporation's future business direction and determined the role of technology in achieving this direction. The project then focused on identifying strategies and specific recommendations to move from the current to future state infrastructure vision.

xwave, in conjunction with personnel from Hydro's Information Systems and Telecommunications (IS&T) department, conducted an in-depth assessment of the existing information technology infrastructure in Hydro through a series of site visits, business and technical interviews and surveys, and detailed data analysis. The approach to the project is summarized in the figure below:



ASSESSMENT	STRATEGY	FOCUS	EXECUTION
Understanding Hydro's current business and technology landscape	Understanding Hydro's future business strategy and the role of technology Understanding what is possible given "state of the art" technology	Identifying specific priorities, from the business and technical assessments, and strategies to move from the current to future state	Developing the ongoing infrastructure program

INTERVIEWS EMPLOYEE SURVEY TECHNICAL SURVEY TECHNICAL INTERVIEWS

Develop research objectives → Identify Sample → Develop Research tools → Data collection → Data analysis

Figure 1 - Project Approach

Using **xwave**'s Assessment, Strategy, Focus and Execution methodology key areas of Hydro's infrastructure were investigated. The areas reviewed are shown in the following figure:

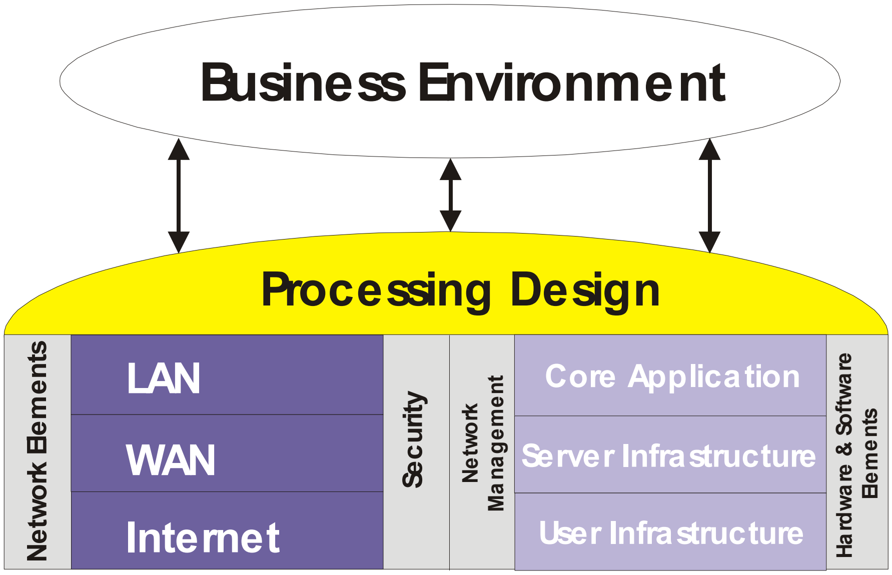


Figure 2 - Infrastructure Assessment Model

Vision

The Vision for Hydro's information technology (IT) infrastructure over the next ten years is defined as follows:

> ***The Hydro Group of Companies will have a single, unified IT infrastructure that manages the core production and support functions in an integrated manner, and that enables all employees to leverage the investment that has been made in the IT Infrastructure by enhancing their ability to perform their job functions***.

This vision depicts a **single view of the network and server infrastructure to manage both the core production and support functions**. As a result of the elevated importance of the entire infrastructure, including that related to support functions, there is a requirement for both additional investment and change in approach. The vision also depicts an increased emphasis on leveraging the IT infrastructure for all areas of its business.

The Vision is based on three fundamental service elements:

- **Seamless Authorized Access:** Employees will have a customized gateway to their information regardless of location or access device;
- **E-enabled Business Processes:** All employees will primarily use electronic means (both low and high bandwidth) to communicate with each other and interact with the system.

- **Integrated Functionality:** The complete business process will be captured and enabled electronically regardless of any organizational boundaries it crosses.

Long-Term Design

Taking the Vision to the next level, a long-term design was developed for the key areas of the assessment (see Figure 2 - Infrastructure Assessment Model). This high level design focused on the 6 to 10 year view and provided guidance for the development of short-term recommendations.

- **Availability and Redundancy:** The long-term design focused on ensuring that there were no points in the infrastructure where the failure of a piece of equipment would cause interruption to the service. This resulted in a network and infrastructure design that provided for multiple paths for data to travel to and from each location, as well as the ability for the server infrastructure to sustain complete loss of any one component.

- **Network Management and Security:** The long-term design also incorporated specific activities and structures to remotely manage its assets from a centralized location, and ensure security and integrity of the data and its operations.

Short-Term Design/Implementation Plan

Using the direction outlined in the long-term design, short-term recommendations were developed for the 1 to 5 year period. This report outlines these recommendations for each of the key areas, and presents the individual projects that have been designed to allow Hydro to implement the recommendations. These projects are coordinated into a single program that can be overseen by Hydro in order to manage the project interdependencies and to ensure maximum efficiencies in implementing the changes to the IT infrastructure.

Projects include:

- Local Area Network
- Wide Area Network
- Internet
- Servers
- End-User Infrastructure
- Security
- Network Management
- Storage Area Network
- Windows Evolution
- Physical Facilities Upgrade

Integrated IT Management Plan

The report also addresses the management and maintenance of the Information Technology Technical Architecture Strategy . It is recommended that Hydro implement an appropriate IT management framework, such as the Information Technology Infrastructure Library (ITIL), to provide structure for each of the management processes necessary for successful operation of the IT function. As well, a schedule of refresh is recommended to keep Hydro's strategy current.

2.0 Introduction

2.1 Background

Newfoundland and Labrador Hydro (Hydro) is a provincial crown corporation engaged in the generation, transmission and distribution of electrical power in the Province. While Hydro is principally a wholesaler of electricity that sells the bulk of its power to an investor-owned utility and several industrial customers, it also sells directly to over 34,000 customers living in rural communities in Newfoundland and Labrador.

In the past 10 years, Hydro has installed several mission critical systems including the Harris Energy Management System, JD Edwards business suite of applications and Lotus Notes. These applications demand a secure and reliable processing and networking infrastructure to ensure all Hydro employees have access to valid and reliable information on-demand.

The Hydro Information Technology Technical Architecture Strategy Project (project) was initiated to identify the strategies and specific recommendations required to achieve a reliable, secure and cost effective networking and processing architecture that provides adequate performance for both the short and long term.

2.2 Objective of the IT Technical Architecture Strategy Report

This report presents key findings and recommendations of the Newfoundland and Labrador Hydro (Hydro) IT Technical Architecture Strategy Project.

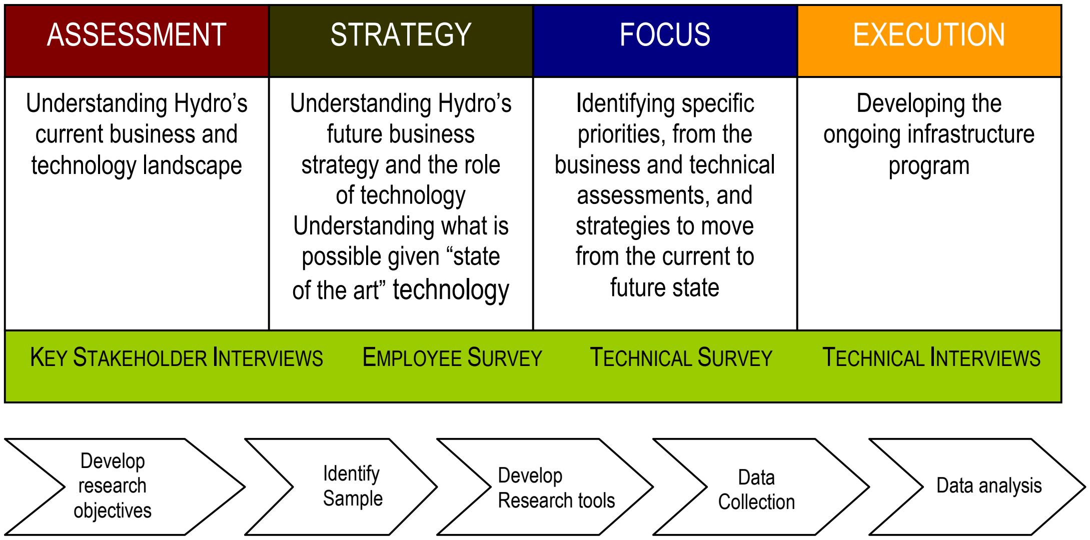
The report summarizes Hydro's current business and technology landscape and future directions, and outlines a long term technical design and short-term recommendations to:

- Achieve a reliable, secure and cost effective networking and processing architecture; and
- Provide a framework for an infrastructure that provides adequate performance over the next 2 to 5 years with a view to 10 years.

The recommendations presented are intended as a source from which Hydro can develop and implement a core technology program. These recommendations strive to balance the potential investment and the reliability issues facing all businesses and meet both technical and financial targets in the short and long term.

2.3 Project Approach

The project used a four-phased approach of: Assessment, Strategy, Focus and Execution.



ASSESSMENT	STRATEGY	FOCUS	EXECUTION
Understanding Hydro's current business and technology landscape	Understanding Hydro's future business strategy and the role of technology Understanding what is possible given "state of the art" technology	Identifying specific priorities, from the business and technical assessments, and strategies to move from the current to future state	Developing the ongoing infrastructure program
KEY STAKEHOLDER INTERVIEWS	EMPLOYEE SURVEY	TECHNICAL SURVEY	TECHNICAL INTERVIEWS

Figure 1 - Project Approach

Four key activities were undertaken:

- **Executive/Key Stakeholder Interviews:** These structured interviews identified the key business drivers impacting Hydro's utilization of the IT infrastructure and how the infrastructure relates to Hydro's long-term business objectives (see Appendix A: Business Needs Research Interview Guides).

- **Employee Survey:** The survey was distributed to all Hydro employees and provided quantitative data on how employees interact with the IT infrastructure in the completion of their daily tasks (see Appendix B: Employee Survey).

- **Technical Survey:** This survey collected information on the existing infrastructure in order to develop the detailed inventory of the current infrastructure including hardware (server infrastructure, routers, switches, etc.), software (application software, office software, etc), and connectivity (LAN, WAN, Internet) (see Appendix C: Technical Survey Questionnaire).

- **Technical Interviews:** These structured interviews validated and completed the information collected in the technical survey and probed further into the technical and business issues faced by the stakeholders in each location.

Each of the key activities required five major steps:

Step 1: Develop detailed research objectives
Develop specific research objectives as the basis for developing the research tool(s).

Step 2: Identify sample
Identify individuals for application of quantitative and qualitative research tools.

Step 3: Develop Research Tools
Develop research tools to fulfill research objectives.

Step 4: Data Collection
Apply the research tool to the identified sample and obtain the associated data to satisfy the requirements of the research objectives.

Step 5: Data Analysis
Analyze and apply quantitative and qualitative data against the requirements identified in the research objectives.

To facilitate the transfer of knowledge from **xwave** professional staff to Hydro staff, **xwave**: involved Hydro *Activity Primes* in all key technology and business information gathering; involved the *Activity Primes* in the development of key recommendations for the business and technical needs assessment through a day-long Vision session; and, provided a best practices database.

2.4 Project Scope

The Hydro project included the review and assessment of current processing and internetworking components of the organization to meet the following objectives:

- Develop a short term (2 to 5 years) enterprise processing and network design;
- Develop a long term (6 to 10 years) enterprise processing and network strategy that will secure the long term business plans of the company;
- Knowledge transfer from the **xwave** team to Hydro staff; and,
- Develop an IT Technical Strategic Plan.

In order to properly understand and assess Hydro's IT infrastructure requirements it was necessary to investigate the various components using a holistic approach. As shown in Figure 2, the scope of the project included: processing design; network elements; hardware/software elements; and, security and network management as well as the related sub-components (e.g. The network elements reviewed were LAN, WAN and Internet).

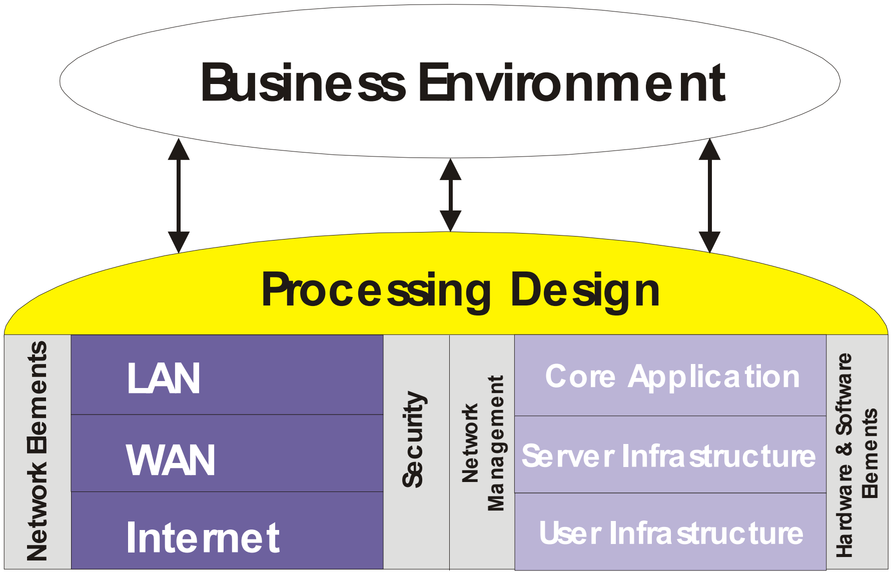


Figure 2 - Infrastructure Assessment Model

It should be noted that while the assessment of existing security infrastructure and the development of recommendations for improving corporate security were within project scope, the development of detailed security policies was not.

2.4.1 Processing Design

As depicted in Figure 2, processing design is the view of how the organization communicates internally, and with the external environment, not on a technology level, but on a business process level. From this view, the business needs can be assessed and appropriate infrastructure put in place to allow the organization to achieve its business goals.

The processing design research included:

- An analysis of the data sources, data applications and associated data flows for core applications including analysis of:
  - Sources data provided to the application;
  - Data provided by the application to the end-user base; and
  - Data provided between Core Applications.

- An analysis of the required supporting infrastructure necessary to maintain the access and availability targets for Hydro including:
  - Enterprise and Local Office server topology; and
  - Supporting network infrastructure.

- An analysis of infrastructure required to support the proposed short-term and long-term future applications identified by Hydro.

2.4.2 Network Elements

The three network elements that were considered in the review of Hydro's IT infrastructure: LAN, WAN and Internet.

LAN
The Local Area Network configuration forms the basis of the infrastructure for an organization, allowing individual end-users to communicate with each other, and with pooled system resources. The investigation focused on core network capacity, routing/switching capabilities, and end-user segment capacity.

WAN
The Wide Area Network investigation included link speeds and methods, protocols, redundancy measures and capacity planning

Internet
The Internet access investigation focused on the access methods, including access speeds, firewalls, and IP addressing schemes for Hydro. In understanding the Internet access requirements, both the technical issues associated with availability and security were investigated, along with the various class of end-user business requirements.

2.4.3 Hardware/Software Elements

The third major area of investigation was the various hardware and software elements. It is important to understand that, as previously noted, the hardware and software elements could not be divorced from the network environment in which they reside, as the two pieces jointly create the infrastructure that enable the organization to function.

Server Infrastructure
The core server hardware and operating system environment comprise the first element in this group. This includes the platform used to host core business applications, as well as support the end-user's access to pooled resources, such as messaging, file and print, authentication, etc. As well, this element includes other system resources, such as Storage Area Networks, backup facilities, High-Availability clustering environments, etc.

Core Applications
There are a variety of core applications that reside on the corporate infrastructure. This is usually the point of interface between the end-user and the IT infrastructure. As a result investigation of the organizations core applications, including JD Edwards and Lotus Notes, was a critical element of the research conducted.

User Infrastructure

The final element is the end-user application and computing platforms that facilitate operation of the business. This is the point-of-entry for users into the IT environment for both office productivity tools, as well as corporate core applications. Items included in the user infrastructure are business productivity tools (Microsoft Office), laptop and desktop infrastructure, collaborative tools, etc.

2.4.4 Security and Network Management

As shown in Figure 2, there are two overriding considerations that must be top-of-mind in the architecture and design of the company's IT infrastructure – security and network management.

Security

Security services are designed to protect the network and user environments from internal and external threats. Areas of investigation included: physical security; firewall policy management, remote access, authentication and authorization, disaster planning and recovery, intrusion detection and action plans.

Network Management

The ability to proactively monitor and manage all elements of the network becomes increasingly important as the use and importance of IT infrastructure increases. Some of the issues investigated in the network management review include: capacity planning; helpdesk resourcing; planned maintenance; and network monitoring probes.

3.0 Governing Design Principles

In reviewing the infrastructure of Hydro there were a number of key principles that were adhered to in attempting to develop a vision of what the end-state infrastructure would look like. Specifically, the following principles were used as the "checkpoint" for the vision:

- The Infrastructure will provide a common user experience regardless of location within the network.
- All users will be able to access their resources from any location, either within the network or outside the network.
- The reliability of the network, for both LAN and WAN, is of paramount importance as the company moves forward to a single, unified network view. As such the design of the network focuses on achieving 99. 99% availability for the LAN infrastructure and 99.9% availability for the WAN infrastructure.
- The infrastructure will be designed with an emphasis on scalability to allow the network to evolve over time as technologies resident in the network change.
- To the greatest extent possible services will be delivered in such a way as to leverage the existing investment in infrastructure
- The Infrastructure design will strive to eliminate duplication of effort by providing a "build once, operate everywhere" philosophy for services.
- The plan will complement other internal infrastructure drivers of Hydro's departments.
- Hydro will encourage its workforce to telework by making access to the applications and data available through remote access.

4.0 Current Assessment

This section of the report deals with the current technology state of Hydro and, as such, is not designed to identify or recommend the changes Hydro should implement to move forward.

4.1 Processing Design

Processing design provides the basis by which the company interacts with its business environment. This includes the various processes for internal systems, operations, supply chain management, etc. that allow the business to function. From this the business needs can be assessed and appropriate infrastructure put in place to allow the organization to achieve its business goals.

Data flow refers to the means by which electronic data enters the system, is captured, processed and stored in its end state. To understand the key elements of the processing design it is necessary to understand data control / information building process from both the front-line and executive levels, including identification of the key data sources and the key data applications.

4.1.1 Core Applications

The Core Applications at Hydro are responsible for the ongoing operation of the enterprise. The primary applications investigated were: JD Edwards, Lotus Notes, Strategy Showcase and the Energy Management System (EMS).

4.1.1.1 JD Edwards

The JD Edwards integrated suite, which is responsible for the major aspects of Hydro's support functions (HR, Finance, Payroll, etc.) was the first core application investigated.

A summary of the data flows is as follows:

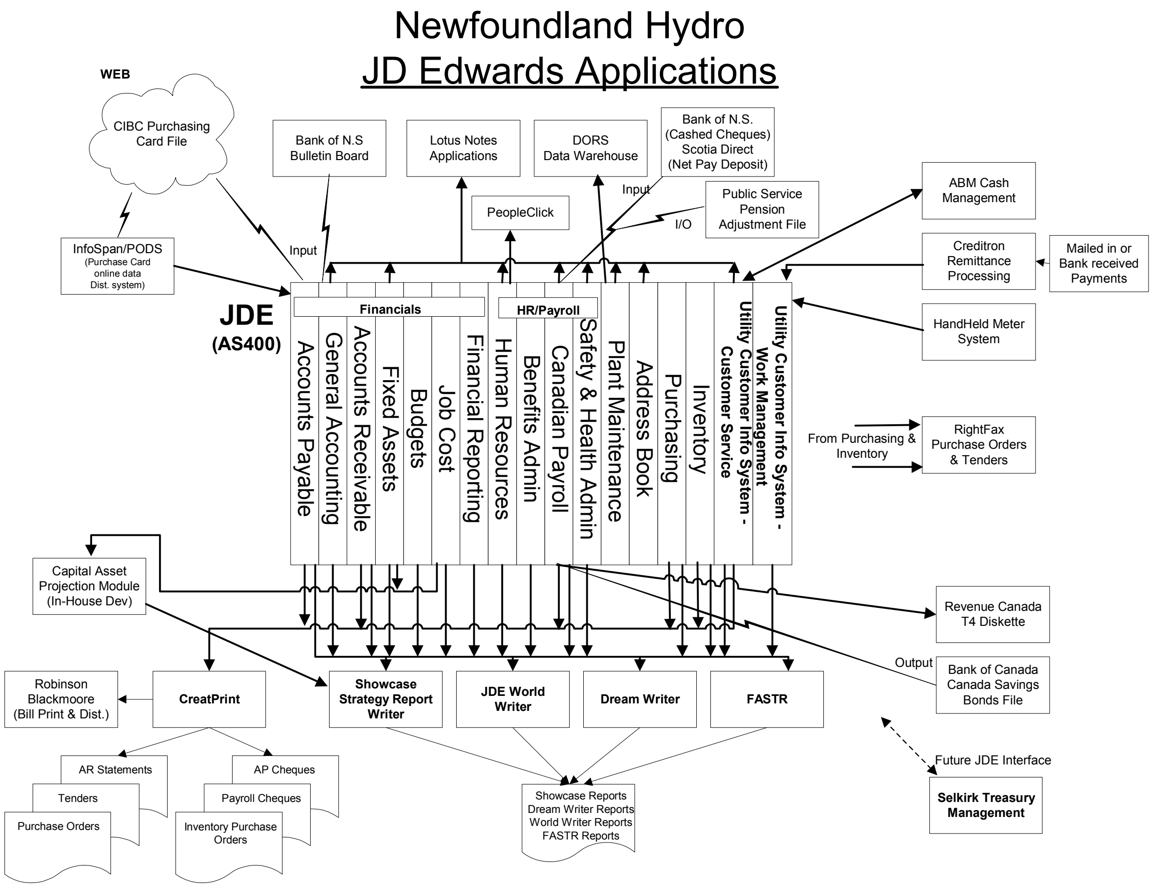

Newfoundland Hydro
JD Edwards Applications
WEB
CIBC Purchasing Card File
InfoSpan/PODS (Purchase Card online data Dist. system)
Bank of N.S Bulletin Board
Lotus Notes Applications
DORS Data Warehouse
Bank of N.S. (Cashed Cheques) Scotia Direct (Net Pay Deposit)
PeopleClick
Public Service Pension Adjustment File
I/O
Input
Input
ABM Cash Management
Creditron Remittance Processing
Mailed in or Bank received Payments
HandHeld Meter System
From Purchasing & Inventory
RightFax Purchase Orders & Tenders
JDE
(AS400)
Financials
HR/Payroll
Accounts Payable
General Accounting
Accounts Receivable
Fixed Assets
Budgets
Job Cost
Financial Reporting
Human Resources
Benefits Admin
Canadian Payroll
Safety & Health Admin
Plant Maintenance
Address Book
Purchasing
Inventory
Utility Customer Info System - Customer Service
Utility Customer Info System - Work Management
Capital Asset Projection Module (In-House Dev)
Revenue Canada T4 Diskette
Output
Bank of Canada Canada Savings Bonds File
Robinson Blackmoore (Bill Print & Dist.)
CreatPrint
Showcase Strategy Report Writer
JDE World Writer
Dream Writer
FASTR
Future JDE Interface
Selkirk Treasury Management
AR Statements
Tenders
Purchase Orders
AP Cheques
Payroll Cheques
Inventory Purchase Orders
Showcase Reports
Dream Writer Reports
World Writer Reports
FASTR Reports

Figure 3 - JD Edwards Applications Data Flow

4.1.1.2 Lotus Notes

An investigation of Hydro's Lotus Notes environment showed in excess of seventy applications. The majority of these applications are client based databases, developed and maintained in house. Approximately seven of these applications retrieve data or submit data to the ERP system, JD Edwards, located on an AS400 at Hydro place. The attached architecture diagram provides a representation of the data flow for the major Lotus Notes databases (See Figure 4).

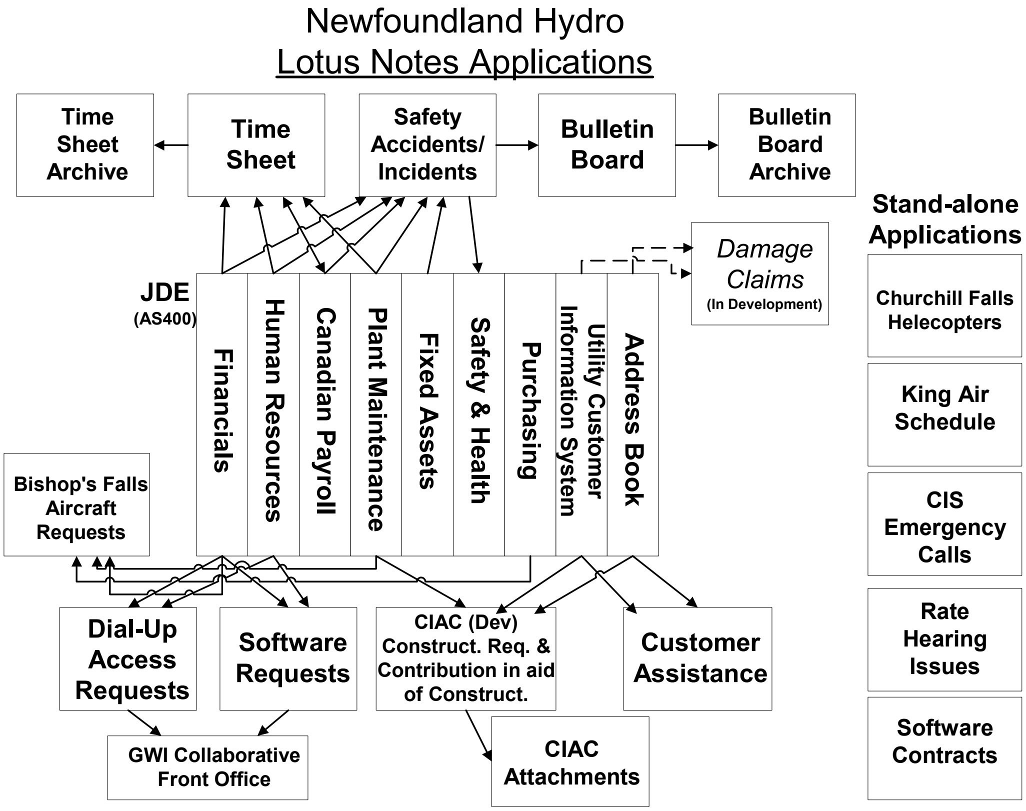


Figure 4 - Lotus Notes Applications Data Flow

4.1.1.3 Harris Energy Management System

The Harris Energy Management System monitors and controls the Hydro Power Grid. Spare parts purchased by Hydro for the customized mainframe environment are stored in the administration systems computer room and entered into a database for easy lookup.

4.2 LAN

4.2.1 Operating System

Hydro has standardized on the Microsoft Windows NT 4.0 server operating system for its application server environment. All users at all locations authenticate to one NT Domain called NLH. Hydro has positioned NT user authentication, and name resolution services at key locations throughout the Hydro WAN to decrease WAN traffic. The NT Primary Domain Controller (PDC) and a Backup Domain Controller for the NLH Domain are located on the Hydro Place LAN. The WINS server is also located on the Hydro Place LAN, it participates in push pull replication with other strategically placed WINS servers at other locations via the WAN.

4.2.2 DHCP / DNS

Hydro uses static IP addressing for servers, routers, printers, switches and other static devices, and DHCP for user IP addressing. The Windows NT 4.0 DHCP service is enabled on one server in each of the Hydro locations. At some smaller Hydro locations with no local server, the IP addresses are assigned statically.

Hydro has an external Windows NT 4.0 based DNS, it is authoritative for the “nlh.nf.ca” Internet domain and is located outside the PIX firewall. This server is also running Microsoft IIS server to publish the corporate WEB site at www.nlh.nf.ca. There are two internal caching NT based DNS servers configured on the Hydro Place LAN. Currently there are no DNS services running at other company sites.

Physical Wiring

The horizontal cable is a mixture of UTP category 3 cable, with category 5 and 5e installed in some locations to support Ethernet at 100mbits. There are also fiber runs between rooms in select locations, used to connect core networking equipment.

Core Switching

The current LAN at Hydro Place utilizes a collapsed layer 2 backbone. The switching infrastructure supports a backplane architecture that scales from 3.6 Gbps to 25 Gbps. Some switches are enabled with Token Ring for interoperability with legacy network protocols.

Access Layer

Users connect via either 4mbit Token Ring over category 3 cable or 100mbit switched Ethernet over category 5 cable. The application servers are all connected via 100mbit switched Ethernet. The AS400 has a 16mbit Token Ring and a 100mbit Ethernet connection to the switch.

IP addressing / VLAN

A pair of non-broadcast Class “B” addresses provide 65,534x2 host address’s for the Hydro place LAN. Layer two VLANS are configured in some locations for the Internet Isolation subnet and the Ethernet class “B” subnet. The Token Ring VLANS are configured to support source route bridging. Routing between VLANS is performed.

4.3 WAN

NewTel Communications, as part of the project team, conducted the investigation of the WAN connectivity. The current WAN infrastructure for Hydro is well documented and as such the internal documentation was used as baseline information in conducting the assessment.

4.3.1 Multiplexers

In order to consolidate the network traffic and maximize efficiency GDC multiplexers are deployed throughout Hydro's network. This equipment is used to carry WAN applications, voice traffic, SCADA & telecontrol information from remote sites to other areas in the network and as well back to Hydro Place.

4.3.2 Routers

As part of the investigation Hydro provided NewTel Communications with an inventory of existing router hardware infrastructure. Hydro utilizes a variety of Cisco router models, ranging from the lower end 1600 series in remote offices, up to a 7200 series in Hydro Place.

4.3.3 Circuits

Hydro's WAN infrastructure is a mixture of dedicated facilities operated over a digital radio network that is owned by Hydro, and leased facilities from Aliant Telecom. The digital radio network is very robust, and has been developed out of necessity arising from the remote locations required as part of Hydro's power generating operations.

4.3.4 Protocols

With the exception of some source-route bridging which is to be eliminated by year-end along with the token ring infrastructure, IP is the only protocol used on the WAN.

The routing protocol currently operating on the Hydro routers is Interior Gateway Routing Protocol (IGRP) and it is understood that there are migration plans in place to upgrade to Enhanced Interior Gateway Routing Protocol (EIGRP).

4.3.5 TMS Network

In addition to its other network systems, Hydro operates a TMS 3000 MUX system. This system is not manageable from an SNMP perspective, and management of the network is further complicated by the use of a text-based system that is not compatible with any other network management system. The TMS 3000 network supports all of Hydro's critical Telecontrol traffic and private voice traffic.

4.4 Internet

4.4.1 Internet Access Topology

Hydro’s current Internet topology revolves around a single point of entry at Hydro Place to the Internet via a10M Ethernet facility to a local ISP. The corporate network is protected by a Cisco PIX firewall. Internet services are distributed to regional offices using leased frame services provided solely for Internet traffic, while administration traffic resides on separate facilities. There are currently no Internet caching servers deployed within the access topology to reduce WAN / Internet consumption.

4.4.2 Remote Access Server (RAS)

Hydro currently has a RAS server at Hydro Place and dial in users call either an 800 number or local number to access the corporate network. At the time of the investigation there was no use of Internet-based VPN to provide access to the corporate network.

4.5 Infrastructure

4.5.1 Servers - Intel

Approximately 60 servers are used throughout Hydro ranging from lower end uniprocessor desktop PCs to larger workgroup UNIX and Intel servers. The PCs generally are used as standalone single purpose servers, or multi-use servers in some remote sites. The larger Intel servers are primarily Hewlett Packard and IBM servers. They are used as Functional (e.g., DNS,WINS) and Remote Office (e.g., File/Print, Messaging) servers.

File and Print servers were recently upgraded in most locations. The standard upgrade included a Hewlett Packard LH3000 with up to two 733Mhz processors, greater than 256MB RAM, normally four 9GB hard-drives configured using hardware RAID-5 and redundant power supplies. Normally, attached to the server is a PowerWare UPS and HP DAT autoloader. In some cases Lotus Notes is also run on the same server. This combination configuration tends to be restricted to very small offices.

Servers are normally configured using vendor-supplied documentation and Hydro developed checklists. As such, all servers should have a very similar configuration thereby making post implementation support easier. Hydro’s latest wave of server replacement focused on a standard configuration by one vendor. Hydro has offices in locations that can‘t avail of tier-1 vendor support. By procuring their own spare parts for this standard server configuration they are able to economically provide their own support and minimize server downtime.

Most locations contain a legacy server running the MAXIMO application. These servers are old and out-dated but a process is in place to retire these and move any required information elsewhere within the Hydro Enterprise.

Depending on the office size and number of people supported by the infrastructure other file servers were present. These servers were generally a few years old and consequently scalability was limited and redundancy non-existent. The functions of these servers tended to be very specific such as print serving, dedicated notes server, application server, etc. The model and specifications of these servers tended to follow a few standard configurations.

4.5.2 Servers - Midrange

Hydro has two RS6000s associated with the Harris EMS. One RS6000 Model F50, named Green, communicates directly with the EMS, collecting real-time data, and makes trending and real-time data available to users in the local area network. In addition, it runs a Hydrometric Data Download, which is a daily dial into the Provincial Government Lands and Agriculture server to retrieve reservoir elevation, precipitation and water flow data. It then inserts the received data into a Sybase historical database.

The second F50, named Blue, runs the Sybase database, making historical report & event information available to users in the Hydro network. The server also runs EMS View that allows users to view real-time and historical control system data with Browser. The server was originally an IBM RS/6000 Model 360 but was recently replaced with the RS/6000 Model F50.

Hydro operates two AS/400 environments, a production environment and a development environment, both running OS400 at V4R5. The AS/400 environment was specifically sized to house the development and production functions for JD Edwards and associated components. Both systems are backed up using BRMS software and 3590 tape drives.

4.5.3 Servers – Capacity

Most of the discs in the servers at Hydro Place datacentre are 10,000 RPM SCSI drives in a RAID-5 configuration. Hydro has developed a policy of purchasing additional disc space for its servers when disc usage reaches 50%. This policy is proactive and prevents shortage of disc space but caution should be exercised to ensure that the disc storage is properly managed.

4.5.4 Servers – High Availability / Redundancy

Hydro has implemented a number of solutions to increase the availability of its servers. Legato Fulltime Cluster is currently deployed on the primary and backup domain controllers, DNS, WINs, and some file/print servers. This product however is being removed in favor of Microsoft Cluster. Microsoft Cluster is current in place for file/print and SQL servers while Microsoft Cluster with Domino Cluster is used to increase the availability of the Lotus Notes servers. In addition redundancy has been built into the server infrastructure in terms of disc space, CPUs, and RAID-5 technology.

4.5.5 Power Protection

The use of UPS's for the orderly shutdown of servers in the event of a power failure is prevalent throughout all of Hydro's locations. Most core components are at least connected to a surge protector.

Non-core infrastructure such as desktops, printers and laptops are often not protected at all and it appears Hydro has not given much consideration to protecting these components.

4.5.6 Data Protection

Hydro has based its data protection on a combination of Veritas Backup Exec and TSM. Veritas is used for backups in remote locations, normally of Lotus Notes databases, and TSM for enterprise backup.

From a procedural perspective, it appeared as if backups were monitored remotely to ensure their successful completion. The extent as to how well backup procedures were followed, especially with regards to offsite storage, seemed questionable as tapes were often left in the server locations.

4.5.7 Software

Software for most servers was based on Windows NT Server as the Operating System, Lotus Notes for messaging, Norton Antivirus for virus protection, Veritas Backup Exec and TSM for data protection. SMS is also widely deployed but this implementation is immature and Hydro has not yet realized it's full potential.

There is no automatic monitoring of software, services, or applications. Ping tests are completed every 15 minutes by ServerAlive software to confirm server presence on the network. Upon failure, email notification is sent to the Helpdesk and System Administrators. Servers containing UPSs use Powerware UPS Monitoring.

Network Management tools used to manage the servers include SMS, VNC (Remote Control software) and standard Windows NT administration resources.

4.5.8 Desktops / Notebooks

Similar to the choice of one vendor for server hardware Hydro has settled on one vendor for desktop and laptop procurement. There are 4 standard desktop/laptop configurations depending on the users requirements. Other, non-standard configurations were present and were either due for replacement or were running legacy applications that did not require much processing power.

The type of software installed on these units varied depending on user function. New installations were based on Windows NT workstation, a Lotus Notes client, MS Office and Norton Antivirus. Desktops and laptops are initially configured using a pre-defined image and further customized when non-imaged applications are required. As before, there is a documented procedure in place and a checklist is provided to ensure a standard implementation.

Power protection is not widely used for these devices. As well, the general organization of power and data wires is not given much consideration.

4.5.9 Printers

There has been standardization on Xerox for large departmental printers and Hewlett Packard for smaller workgroup printing.

4.5.10 Data Centers / Server Rooms

Server rooms were often multi-purpose rooms, with servers sharing space with network, telecommunications and general office equipment. Servers and other core infrastructure are often in high traffic areas such as corridors or photocopier rooms. Server location appears to be determined by space availability and is not given high priority.

The use of racks for server hardware organization is minimal. General organization and tidiness of Servers, UPS's and other server hardware is inadequate. Wiring management and organization for both data and power is not widely used. Locations that recently had data wiring upgrades tended to follow an unofficial standard and make use of good wiring management practices.

Most data center and server rooms showed a general untidiness with books, old hardware, spare parts, retired or faulty equipment, etc. lying about.

Proper server racks are rarely used, further adding to the disarray in most server rooms. Additionally, each server normally has it's own monitor rather than making use of a KVM switch thereby adding more hardware to an already unorganized environment.

The Hydro Place datacentre is owned by Hydro and managed by its employees. There are signs on the doors to the datacentre. The room has three access points – one in the front of the datacentre, one in the rear and one leading out into the System Administration area. Inside the datacentre the equipment sits upon a raised floor. The room is not filled to capacity and there is potential room for growth. The datacentre is partially carpeted which increases the level of dust particles and increases the chances of static electricity interfering with the servers. In addition, carpeting makes it more difficult to get into certain areas underneath the raised floor.

The Hydro Place data center is supplied by two 100Amp feeds from Newfoundland Power. In addition, there is a diesel generator backup system for the entire building that requires approximately 7 seconds to initiate in the event of a power loss. Color-coded outlets in the data center identify power sources that are supplied by the diesel generator. Review of the data center environment showed that all server equipment was connected to appropriate outlets.

From an Uninterrupted Power Supply (UPS) view, the datacentre currently has a steady-state power draw of approximately 11 KVA. UPS is provided on an individual basis for each server using a stand-alone UPS's designed to bridge the 7 second interval between power loss and the diesel generator coming online, or provide for a graceful shutdown period in the absence of diesel-powered backup.

A review of fire suppression showed a two stage dry-pipe system.

Currently the Hydro Place data center environment uses two air conditioning units on a manual control. Similarly, the A/C units are not linked to an automatic stabilized temperature control unit. Instead, visual thermometer readings are used. Hydro has HVAC humidity monitors installed to avoid over cooling. Separate venting for the Datacentre than for the broader building is preferred, as is currently provided in the Hydro Place location.

4.6 Security

4.6.1 Domain Access & Logon Security

No strict cryptic domain password policy is enforced although passwords are required to be changed on a rotating basis. Some servers inspected were logged in with administrator rights.

While laptop users are provided lockdown mechanisms for their machines there was very sporadic use of the devices. Screen-saver passwords are not used during times when the machines are left unattended.

4.6.2 Standard Workstation Operating System Images

xwave performed a limited vulnerability assessment of all workstations in selected sites. Hydro has deployed a standard OS and application image to network clients and therefore the sample data should be a fair indication of workstation vulnerabilities across the corporation. It is important to qualify this statement by noting that software installation restrictions are not enforced by Hydro and therefore slight variations in scan results will occur. Almost all workstations scanned reported the same types of problems with missing patches and non-administrator permissions. The vulnerability assessments performed did not include susceptibility to DoS attacks as this type of scan almost always crashes the target device several times and **xwave** performed these scans during business hours. This means that the tests are not all-inclusive and do not report on problems that would be discovered during an invasive test.

There is no mechanism in place to control the mutation of the standard image. That is, although equipment is provisioned with a standard image of software, once the user has the machine they are at liberty to add, delete or modify the software configuration.

4.6.3 Standard Server Configurations

Servers tend to have more distributed purposes and are therefore not fully standardized on a particular image. Based on **xwave**'s research, the remote office multipurpose servers are very close to being identical at remote locations. As well, a standard installation guide provided by the vendor has been followed which gives a good base from which to start with.

4.6.4 Internet Accessible Services

Hydro's DNS/Web server currently resides on the e1 interface of the external Internet router (outside the PIX firewall). That is, it is fully accessible from the Internet without any protection provided by creating a DMZ using the existing PIX firewall.

An access-list has been applied on the external router to restrict traffic to specific public servers on the public segment. Although blocking of unwanted traffic to several public addresses has been implemented, it has been found that this access-list does not restrict traffic to the rest of the public address block due to a final permit any statement. This statement reduces the effectiveness of a previous statement allowing established traffic only to this segment.

4.6.5 Internet Gateway

4.6.5.1 Firewall Type and OS Version

The current PIX Firewall is version 4.4(7), which is significantly out of date although it is understood by **xwave** that a hardware limitation is keeping the version from being upgraded immediately.

4.6.5.2 Current Firewall Security Policy

The current PIX firewall security policy was reviewed with a view to identifying potential security holes or lapses.

4.6.6 Internet Mail System

The current SMTP forwarding services is located off the internal Lotus Domino SMTP Server, inside Hydro's firewall. **xwave** performed a limited vulnerability scan against the current public SMTP gateway. The vulnerability assessment performed did not include susceptibility to DoS attacks as this type of scan almost always crashes the target device several times and **xwave** performed this scan during business hours. This means that the tests are not all-inclusive and do not report on problems that would be discovered during an invasive test. The results of this scan include several potential vulnerabilities related to piping mail output to the local file system or program. Also included in this scan report is the remote Winframe server. No vulnerabilities were discovered for this device but again, a full invasive scan was not performed.

4.6.7 Outbound Authentication and Logging of Internet Access

Hydro controls Internet access by restricting the list of subnets that are allowed to start outgoing NAT connections at the PIX firewall. Hydro does not employ a Proxy Server to manage access based on NT Domain user account.

4.6.8 Remote Access

4.6.8.1 Modems Attached to User Workstations

Numerous modems were attached to user workstations, and the noted workstations were not specifically configured to disable dial-in. That is, a user may use a modems to connect to the local ISP with personal accounts to check e-mail. Although almost certainly not intentional, this represents a full bypass of the Internet firewall security policy, as users would almost certainly remain connected to the corporate LAN while doing this.

4.6.8.2 Dedicated Dial Solution

Hydro currently has a RAS server at Hydro Place and dial in users call either an 800 number or local number to access the corporate network. During the initial security review, users were authenticated using a status username and password scheme. Before completion of this report, the plan was implemented to perform authentication using the SecurId system, which drastically improves the level of security confidence in the system.

4.6.9 Anti-Virus Configuration

All clients and servers on the corporate network are configured with Norton Anti-Virus solution that allows for frequent, easy to apply updates.

4.6.10 Logging and Log Data Presentation

Currently Hydro performs some manual log review of activity on the PIX firewall, but this is performed only in an ad-hoc basis, and not proactively. No logging is performed on an application basis, with the exception of AS/400 logs, which are generated and summarized on a daily basis.

4.6.11 Active Intrusion Detection

There is currently no active Intrusion Detection System in place at Hydro.

4.6.12 Configuration and Change Management

Configuration and change management for Hydro’s server, desktop and AS/400 infrastructure is currently handled independently. As well, there is no online data repository of configurations and change management procedures for maintaining Hydro’s IT assets. There is also no Change Management Coordinator for Hydro.

4.6.13 Disaster Recovery and Business Continuity

Hydro is currently involved in drafting a high-level Disaster Recovery and Business Resumption Plan.

4.7 Network Management

4.7.1 Network Elements

4.7.1.1 Switches, Routers and Hubs

The WAN is monitored during business hours using Cisco Works 2000. The Cisco Works platform is housed on a single NT server and is set up to monitor the WAN and LAN hubs, switches and routers using Cisco SNMP information. This allows Hydro to view a large portion of its network, with the exception of areas where bridging is used to move from Ethernet to token ring networks, and selected hubs in smaller locations that are not SNMP enabled.

SNMP works in such a way that when an event happens a signal is triggered to a centralized console. This event may be the failure of a device or component, or the reaching of a threshold. Currently the SNMP configuration only checks for device failure, and not thresholds such as CPU or memory utilization. The Cisco Works platform also allows Hydro to remotely administer the network elements to provide firmware and configuration updates.

Given that Cisco Works is currently being evaluated there are no regular reports generated for proactive monitoring or capacity management.

4.7.1.2 Circuits

From a circuit perspective Hydro has a mixture of privately owned digital microwave radio circuits and a variety of leased line circuits procured from NewTel Communications. Currently the NewTel circuits are managed by the provider using a combination of HP Openview and its Concord Network Health platform. The private digital radio network operated by Hydro is managed using HP Openview. The Openview system is monitored from a stand-alone server console with no integration into the CiscoWorks platform used to monitor the network elements. The stand-alone server console is monitored on a business hours basis and collects information on basic circuit up/down status. There is no performance monitoring or measurement on the network to measure congestion, latency or other performance related variables.

4.7.1.3 Internet

As discussed in the Internet portion of the investigation, Hydro currently receives its Internet connectivity through a single point of access from Rogers Cable (Rogers). At this point in time Hydro does not receive any performance information from Rogers on up/down performance, latency, or throughput.

4.7.2 Infrastructure

4.7.2.1 NT Servers

As of this report there was little or no monitoring tools in place at Hydro to cover its NT server infrastructure. Currently Hydro uses a program called “Server Alive” to ping each server on a fifteen-minute interval to record up/down status. The information from the Server Alive program is used to generate automatic e-mails to the helpdesk when a server does not respond with the helpdesk operating on a business hours basis. SNMP is not enabled on the server infrastructure to capture trap information and alarms such as exceeding thresholds or failure of components such as network adapters, etc. In addition, there is no monitoring of file system capacity, network collisions (which may be due to a faulty network adapter), memory utilization, CPU utilization or other parameters on any of the servers identified.

4.7.2.2 AS400

The AS400 environment is more closely monitored through daily reports generated tracking a series of variables on a subsystem level. Specifically, a daily report is generated using fifteen minute intervals to track elements such as transactions, response time, CPU utilization, disk I/O, etc. The report creates an automatic summary table that rolls up information from each of the subsystem reports. Once the report is created and printed, a manual review is done to identify key system parameters, such as the CPU spike, average utilization, etc., and information is hand-written on the report. The paper copy is then filed for future reference if required.

In addition to performance monitoring, the AS/400 can be SNMP enabled, though at present it is not enabled nor monitored.

4.7.2.3 Desktop Infrastructure

Hydro is using Microsoft SMS as a tool for managing licensing on desktop infrastructure and selected use by the helpdesk to take control of end-user PC’s for troubleshooting. SMS is being tested for use in pushing system and configuration updates to the desktop. Local load points for software have been established at remote sites to make the process more efficient. As well, HP Standard Desktop Tools are being used by the Help Desk for desktop support.

4.7.3 Applications

There are currently no application-specific agents in place for the Core Applications of JD Edwards, Strategy Showcase and Lotus Notes.

4.7.4 Environmental Monitoring

Currently there is limited environmental monitoring, mainly for the digital radio network. HP Openview is used to remotely monitor the Microwave Radio system. Environmental monitoring, at the device layer, is difficult to implement because not all vendors embed environmental monitoring intelligence into their products. The only other alternative is to implement environmental monitoring systems for the physical locations in which mission-critical IT infrastructure is housed. This can be extremely cost-prohibitive if the IT infrastructure is widely dispersed, both geographically and within a specific office.

5.0 BUSINESS NEEDS RESEARCH

This section presents a summary of the business needs research portion of project. This portion of the project involved a review of Hydro's current business and technology landscape, identification of the Corporation's future business direction and, the determination of the role of technology in achieving this direction.

5.1 Approach

Information for the business needs research was collected through personal interviews with the executive and key business stakeholders and the survey distributed to all employees.

5.1.1 Executive/Key Stakeholder Interviews

The purpose of the interviews was:

- To understand, from the perspective of key stakeholder groups, the major technology, business and political issues that are driving the growth and continued operations of the Company.

To fulfill this purpose, more specific objectives were developed and used to prepare standard interview guides that were used to prompt discussions.

5.1.2 Employee Survey

The second research method used for the business needs research was an employee survey. The purpose of the survey was:

- To understand how the employee base of Hydro currently utilizes the IT infrastructure and its associated support functions; and

- To understand the required characteristics of the IT infrastructure to support the employees in conducting their job functions.

A sampling plan was designed using a sample of 850 e-mail addresses, with a target response rate of 50%, or 425 completed questionnaires. In addition, 350 abbreviated paper surveys were distributed to employees who did not have access to e-mail.

The employee survey had 550 respondents, which is an impressive number given the relatively short timeframes involved. From a statistics point of view, given the level of responses in each of Hydro's business units, we are 95% certain that the answers given are accurate to within 4.8%.

5.2 Findings: Executive/Key Stakeholder Interviews

5.2.1 Business Direction and Vision

Interviewees indicated that over the next five years, Hydro will adhere to its core lines of business (generation, transmission & distribution). The overarching goal of the organization will be to continue to produce the lowest cost reliable power in a way that mitigates environmental impact and fosters a safe workplace. As well, there will be a continued focus on reducing costs and enhancing employee productivity.

It was also noted that Hydro will be investigating non-core business opportunities to increase revenue.

5.2.2 Key Business Drivers

When asked to identify the key drivers for Hydro's business, interviewees tended to frame their responses based on their operating division within the organization. Notwithstanding, there were a number of common themes that emerged.

- **Cost Structure:** Interviewees indicated that Hydro faces the challenge of managing a cost structure where significant costs, such as fuel, are outside of its control, while other costs, such as interest carrying charges, can be managed to a limited extent.

- **Regulatory Framework:** Interviewees indicated the level of regulatory reporting has increased substantially since Hydro became a "rate regulated utility" in 1996. The outcome of rate hearings has a direct impact on the organization's future financial performance and therefore the regulatory framework is a key business.

- **Environmental Impacts:** In fulfilling its mandate, Hydro has a significant impact on the natural environment, from redirecting rivers to construction of transmission lines. Therefore, Hydro must be, and must be seen to be, operating in a way that minimizes its impact on the environment.

- **Demonstrate Value:** Interviewees indicated that Hydro must demonstrate, to its shareholder and the public, the economic and strategic value it provides through its role in the generation, transmission and selected distribution of power.

5.2.3 Major Organizational Challenges

Interviewees identified five major organizational challenges facing Hydro:

- **Identify efficiencies and streamline processes:** To address this challenge, interviewees identified the need to review business processes and potentially redesign some of the core activities in the company.

- **Optimize Performance:** Interviewees noted the need to optimize the value of both corporate and physical assets. Further, it was noted that managing performance will require the identification of standardized performance metrics, related tools and processes.

- **Continuity of Service/Succession Planning:** In light of the large number of potential retirements (25% of the workforce will reach retirement age in the next five years) interviewees agreed with the need to ensure retention of corporate knowledge while fully exploiting the opportunity for culture change.

- **Culture and Image:** Evolving the corporate culture to place increased emphasis on communication and morale building was identified as a key organizational challenge.

5.2.4 Operational IT Issues

Interviewees also presented their views on the operational issues within Hydro that IT was either addressing now or could be addressing.

- **Data and Information**

In general, the quality and timeliness of data being collected by the organization's information systems is deemed to be satisfactory. However, a number of issues concerning the location, input and extraction of that data were identified. A second issue was raised concerning accessing data, especially within JD Edwards, and pulling information together from disparate sources. This task often requires manual processes, which may include the transposition of data multiple times. Finally, interviewees indicated that they would like to receive information proactively. At present, information has to be 'pulled' from sources, formatted, and then sent to the requesting party. There was support for having pre-defined data and information 'pushed' to users (reports & dashboards of information accessed through an Intranet).

- **JD Edwards**

Two key issues were identified with JD Edwards: the user interface and reporting. The current implementation of JD Edwards is a "green screen" or terminal emulation technology. Users indicated they were having difficulty adapting the relatively intuitive Windows interface functionality to the legacy application. This causes greater difficulty for infrequent users who have trouble with navigation within the system. From a reporting perspective, the JD Edwards system has not been tuned to produce paper reports and related documents. Interviewees also indicated that using the Strategy Showcase reporting tool has also been problematic, given the transactional nature of the system. Users typically experience difficulty in rolling up information to a summary or drilling down to appropriate detail levels.

5.2.5 Opportunities for IT

Interviewees were also asked their views regarding the opportunity to leverage Hydro's investment in IT to create additional value. It is important to note, however, that these opportunities represent *perceived* opportunities as identified by the interviewees.

- **Business Process Review**

The first area identified by the interviewees was a business process review and potential redesign. While it was identified as primarily a business issue, it was thought that IT would be able to build or refine the enabling and supporting technologies. The business process review was viewed as a driver for obtaining cost efficiencies and breaking down organizational silos. It was also noted that it would provide a foundation for workflow and automated business processes (e.g. Automated cross-business unit integrated planning).

- **Building the Data Warehouse**

A second opportunity identified by interviewees was the development of a common inventory of data, tools and processes owned by the organization to provide support for management information and decision support systems. A Data Warehouse would also support production of Key Performance Indicator information and provide a common repository of data for events such as rate hearings. Another view of the Data Warehousing opportunity was that it would have the potential to separate production/transactional systems from reporting systems.

- **Enhance Remote Monitoring and Management**

Enhancing remote monitoring and management for portions of the power distribution infrastructure, such as substations, was also seen as an opportunity. It was also felt that using remote monitoring and management would build capabilities to collect environmental data and indicators, which could be integrated within a data warehouse application.

- **Support for Internal Communications**

  The subject of internal communications and culture and how IT can impact, and is impacted by, was raised throughout the interviews. In general, it was felt that Hydro could use Intranet technologies to support internal communications in areas such as employee self service (personnel data), employee satisfaction surveys, information dashboards and information push technologies and personnel directory information.

- **Support for eLearning**

  In conjunction with the opportunity presented by the Intranet, it was felt the same technology could be leveraged to support eLearning initiatives, such as new recruit orientation, ongoing training and material refresh and apprenticeship training (in conjunction with Technical Schools). Interviewees commented that by using an eLearning approach, Hydro could deliver a consistent base of training and learning materials to employees, irrespective of time or place, in a cost effective manner.

- **Support for External Stakeholders**

  Several interviewees noted that similar to the way an Intranet provides for internal communication, there exists potential for an extranet to allow Hydro to communicate with its external stakeholders. Under this approach, the extranet could be used to provide required reports to stakeholders such as the Public Utilities Board or the Department of Mines and Energy, and as a mechanism for supply chain management through eProcurement and B2B initiatives.

- **Records & Document Management**

  Interviewees also felt there was an opportunity to provide processes and technologies to support the management of documents through the life cycle of creation, use, archive, and disposition. It was felt that the use of a document management solution would support retrieval and sharing of records and documents and would provide a means to maintain corporate continuity in the face of potential large-scale retirement of senior, experienced personnel.

- **IT Strategy, Governance & Change Management**

Interviewees also felt that there was an opportunity for development of an IT strategy, governance and change management to align IT investments with business needs and priorities. It was noted that this approach would help identify projects, define priorities, secure funding and management commitment through a multi-year process.

5.3 Observations and Conclusions: Employee Survey

5.3.1 Key Business Issues

Business Process	Issue
Application and Network Availability	Almost ½ of users indicated that applications or the network was down when they need it
JD Edwards	Not leveraged as the powerful tool it is - many users feel it is difficult to use but believe it contains the information they need. Some functionality issues in select groups.
Security	Significant number of users connecting from outside their office suggests VPN solution may be required. Multiple passwords suggests use of a token for multiple system authentication. Selected concerns over security of sensitive data
Training	Many users feel insufficient training has been provided in JD Edwards. Reluctance to use CBT - preference for classroom and workshop settings
Help Desk	Considerable self-help is used (F1 key, Internet searches). Excellent problem resolution for Network connection, Passwords and Hardware/Software issues

5.3.2 Home Technology Use

- **Proficiency/Familiarity:** The majority of survey respondents (66.9%) indicated they considered themselves Intermediate users and a further 8.8% considered themselves Expert users. Approximately 81% of respondents also indicated that they had a personal computer in their home, with Labrador and Hydro Place respondents indicating the highest percentage ownership.

- **Internet Access:** Approximately 70% of respondents indicated they have some form of Internet access at home, with the majority (42%) having dial-up access. From a demographic perspective, the Professional and Management groups tended to have a higher percentage of Internet access and the Maintenance group had the lowest. Of the

30% of employees who indicated they did not have Internet access from home, almost half noted that they did not have a computer at home, precluding access. For those users who have dial-up Internet access to the Internet through Hydro's network, a VPN solution may provide additional security.

5.3.3 Office Technology Use

- **Computing Platform:** The majority of respondents (56%) indicated they used a desktop PC at work. Approximately 6% use both a desktop PC and a laptop in their office location.

- **Internet Access:** Of these users, 86% have Internet access at work through Hydro's corporate network. Employees conduct a number of job related activities on the Internet, with the most popular being Research (34%), Technical Support (27%), Users Groups (12%) and Training (12%).

- **Personalized Home Page:** Only 17% of Hydro Internet users have ever "personalized" a home page on the Internet. There was a high correlation between this question and the technical familiarity of the Hydro user, as well as whether they had Internet access from home.

5.3.4 Corporate Network

The set of questions ascertained the level of interaction between users and the network, both from their main office location, as well as remotely.

- **Network Access:** Approximately 53% of employees accessed the network more than 20 times during the last month. . The highest percentage of responses came from Professionals, members of the Finance and Production groups and primarily Hydro Place employees. Only 7% of the employees had not accessed the network at all. Though this number is small, it still represents a barrier to the deployment of e-enabled business tools that can lead to efficiencies.

- **Remote Access to Network:** Some 53% of employees do not connect to the corporate network from home. The remaining 47% vary from a few times to more than 10 times. With 47% accessing the corporate network from home, Hydro should review the usage of a VPN to secure corporate data. Potential exists for unauthorized access to the corporate network, given the present level of access.

- **Network Speed:** The majority (80%) of employees feel the network does not prevent them from completing their job in a timely manner. While 78% of users responded that the network speed was acceptable, employees in Western Newfoundland and in Labrador tended to disagree, indicating speed issues on their network segments. Further, approximately 47% of respondents perceived there are times when information is required but the network or an application is unavailable. This seemingly contradicts the responses in the earlier question concerning the speed and inhibiting features of network access. Investigation has confirmed that when the network and applications are available, the speed is acceptable.

5.3.5 Software Application Use

- **Application Use:** The primary applications used by Hydro employees are Microsoft Office suite of products (Excel, Word, PowerPoint and Access) and Lotus Notes applications. Lotus Notes accounted for 41% of employees network usage, while JD Edwards (20%), Internet (17%) and Shared File access (11%) highlight the other primary network accesses.

- **J D Edwards Feedback:** A number of questions were directed at the perceived level of functionality and contentment with the JD Edwards suite of applications. Approximately 72% of employees responded that they did not have to modify data once it is obtained from JD Edwards. Supporting this is a follow-up question in which 44% of employees feel that JD Edwards does not provide all the functionality they require to complete their job. In terms of data and information in JD Edwards, 44% of respondents indicated the suite provided them with the information they require to complete their job.

- **Training:** Only 25% of users felt they had received an appropriate level of training for JDE. For the Microsoft Office suite of products, a majority of respondents (64%) did indicate that appropriate Lotus Notes training had been provided. The Western and Labrador groups tended to disagree strongly, indicating that they had not received adequate training in either of the two tools.

5.3.6 Technical Support

- **Help Desk Usage:** Of all respondents, only 25% indicated that they had not used the Help Desk at all during the past month. The majority of users (56%) had contacted the Help Desk 1-3 times. When asked the reason for their calls to the Help Desk, Unable to Access the Network was the most significant answer (21%).

- **Help Desk Satisfaction:** Three quarters of respondents indicated that they received appropriate and timely responses. 55% of employees indicated they had seen an improvement in the performance of the help Desk in the last 12 months.

- **Training Approach:** Users were evenly split when asked whether they would like to access training material over the company network on their own schedule. A follow-up questions confirmed that users still prefer a classroom or workshop setting for training on software applications.

5.3.7 Security

- **Passwords:** 72% of users tended to respond that there were too many passwords to remember, prompting them to write them down or used applications that keep track of passwords.
- **Access:** The majority of users (81%) also indicated that they have all the access privileges necessary to complete their work. Though this is a high percentage, the remaining 19% feel that they are restricted from using system resources that they deem necessary to complete their work.

- **Security Appropriateness:** Concerning overall Hydro systems security, 78% of respondents agreed that security checks in place adequately protect data.

5.3.8 Demographics

The final section of questions asked a series of demographic questions that were used to further analyze the responses. A total of five pure demographic questions were asked. The following tables summarize the data:

General Job Function	
Executive / Director / Manager	7 %
Professional (Engineering, Accounting, IT, etc.)	30 %
Front Line Supervisor	13 %
Clerical	16 %
Maintenance	22 %
Other	11 %

Division	
Transmission and Rural Operations	32 %
Finance	12 %
Production	29 %
Human Resources and Legal	6 %
CF(L) Co.	21 %

Gender	
Male	78 %
Female	22 %

Location	
St. John's	40 %
Holyrood	7 %
Whitbourne	1 %
Happy Valley	2 %
Wabush	1 %
Stephenville	2 %
Deer Lake	2 %
St. Anthony	3 %
Port Saunders	4 %
Churchill Falls	21 %
Bay D'Espoir	8 %
Bishop Falls	8 %

Years of Service	
< 5 years	19 %
5 to 10 years	9 %
11 to 15 years	25 %
16 to 20 years	14 %
21 to 25 years	17 %
> 25 years	15 %

6.0 Architecture Vision

6.1 Vision

The vision articulates the function of the IT infrastructure in an ideal world over the long term (circa 2010). The vision was developed to reflect best practices and trends in technology and the key business drivers and directions of Hydro. This vision should be understood and accepted as a benchmark against which current and future investment can be assessed.

With this in mind the Vision for Hydro's IT infrastructure is defined as follows:

> *The Hydro Group of Companies will have a single, unified IT infrastructure that manages the core production and support functions in an integrated manner, and that enables all employees to leverage the investment that has been made in the IT Infrastructure by enhancing their ability to perform their job functions.*

There are two key elements addressed in the vision:

- **A single, unified IT infrastructure:** Currently the Energy Management portion of the system is in a silo from the remainder of the infrastructure due to the importance of the task it performs. However, field staff, engineering services, production, transmission, and distribution personnel are increasingly reliant on information and communications provided by the support infrastructure. As a result, the availability of network resources has a direct impact on the ability of Hydro to deliver on its primary mandate and in the future state, the availability of the entire infrastructure is raised to the same level as currently provided for the core production environment. *This will require a significant change in approach and expenditure on these elements to create this unified view.*

- **All employees leverage the IT investment:** The second major facet of the vision revolves around the way in which Hydro's employee base interacts with the system. In the future state, business functions must be performed in a manner that leverages the investment in IT infrastructure for all areas of its business. The IT process can no longer be segregated from the business process; *they are one in the same.*

6.2 Service Elements

Taking the vision down to the next level the architecture vision of the Hydro group of Companies is based on three fundamental service elements.

- **Seamless Authorized Access:** It is proposed that, from a service perspective, the IT infrastructure will be able to detect who is attempting to access the system and provide them with a customized gateway to his/her information regardless of location or access device. In the future, while it is possible to have multiple repositories of personal data it is necessary that there be a single integrated source for personnel data within the company that drives these repositories.

- **E-enabled Business Processes:** Under the proposed vision all employees will primarily use electronic means (both low and high bandwidth) to communicate with each other and interact with the system.[1] That is, the current mosaic of processes will be replaced with an integrated E-enabled business process that is focused on capturing the data at its source electronically, and then consistently tracking that data through the system to its end state.

- **Integrated functionality:** It is viewed that the IT infrastructure will be designed in an integrated fashion such that the complete business process is captured and enabled electronically regardless of any organizational boundaries it crosses. The concept is to provide input into the system only one time for each item, and have all the associated "ripple effects" of that input automatically associated with the new information.[2]

In conjunction with the above three elements there is also a requirement for establishing an ongoing method of managing the IT infrastructure in such a way that coordination across the entire base is easily achieved and centrally controlled. As such, the vision would include the implementation of an IT management process to incorporate various elements of operational and tactical management, such as using Service Level Agreements for managing costs, a centralized change management function, etc. The topic of ongoing management is further addressed in Section 9.0 – Integrated IT Management Plan.

[1] This drive to an electronic interface will take the form of three major thrusts: active pursuit of wireless implementations; centralization of processing through pushing thin client technology; and, the exploration of new devices and methods, such as speech recognition, wearable computing and handheld devices for data input and output.

[2] Under this scenario the field technician would receive a work order electronically, complete the work order and close it out electronically. When closed, that work order would automatically register back with the originating source (such as a routine maintenance schedule), a timesheet for recording time, the inventory and purchasing system for updating inventory counts, the financial system for capturing maintenance cost on a piece of equipment, and so forth.

7.0 Long-Term Technical Design

The next step in establishing direction for Hydro is to identify a specific technical design vision, first for the long term (greater than 5 years) and then bringing the vision back to the short term (less than 5 years), and finally back to immediate actions that can be taken to help Hydro progress towards the desired end-state. To facilitate this the same major categories will be used as those in the technical assessment.

Generally, the number of users accessing various corporate applications is the biggest driver of infrastructure requirements in the areas of LAN, WAN, Internet, Servers and End User devices. The size of various company locations results in a consistent architecture based on "Class of Office". For the purpose of this report, the following describes the various classes of office as diagramed in Figure 5 - Hydro Long Term Technology Architecture:

- **Hydro Place Data Centre** – This location is the core of Hydro's computing environment hosting major corporate applications and providing connectivity to over half the company's users.

- **Large Office** – These are large sites with greater than 75 users. The sites that fall into this category are Bishop's Falls and Churchill Falls.

- **Medium Office** – These are medium size sites with between 26 and 74 users. The sites that fall into this category are Holyrood and Bay D'Espoir.

- **Small Offices** – These are small sites with 25 or less users that have connectivity to the corporate WAN. The sites that fall into this category are Whitbourne, Stephenville, Port Saunders, St. Anthony, Deer Lake, Wabush and Happy Valley.

- **Remote Offices** – These are company locations that do not have connectivity to the corporate WAN and must use remote access methods to utilize corporate applications. These sites include all remaining office, depot, substation, home access and mobile user locations.

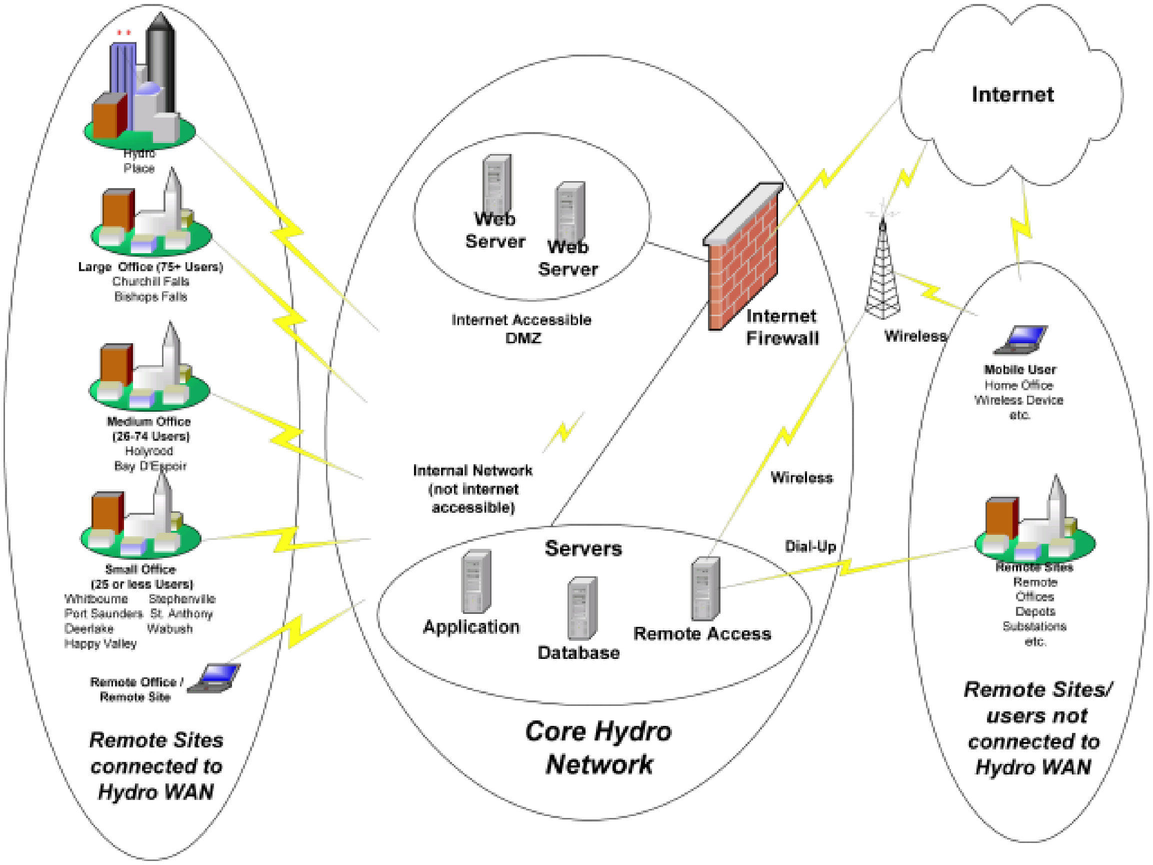


Figure 5 - Hydro Long Term Technology Architecture

7.1 LAN

There are five main elements to consider in the long-term LAN technical design:

- Core Backbone capacity,
- Desktop capacity,
- VLAN's,,
- Performance Enhancements,
- Availability and Redundancy

As described in the Vision, Hydro is to become a fully **E-enabled business**, with its employees using the IT infrastructure as their main method of communicating with the enterprise and each other. To accomplish this, the IT infrastructure must be able to provide the bandwidth needed to deliver data-intensive applications out to the user base despite the fact Hydro will continue to operate in a widely geographically dispersed environment. There will be resultant pressure on the IT infrastructure to meet the dual responsibilities of richness of experience and efficiency. The LAN infrastructure will need to be able to support varied future multimedia applications in the network such as Voice over IP, Desktop Videoconferencing, as well as delivery of productivity applications such as JD Edwards and Data Warehousing. The long-term technical design dictates that the core backbone LAN infrastructure must support a multi-Gigabit switched environment (vertical) as the enterprise moves to become fully E-enabled as described in the vision. This would be coupled with providing a minimum 1 Gigabit switched Ethernet connectivity over copper. As well, the implementation of wireless LAN connectivity would be expanded to include hotelling offices, conference rooms, executive floors and other areas where mobile connections would be beneficial.

Another area of impact that the Vision has on the long-term technical design is in the area of Virtual LAN's (VLANs). VLANs can be viewed as a group of devices on different LAN segments which can communicate with each other as if they were all on the same LAN segment. To accomplish this the long-term technical design includes full implementation of a dynamic VLAN environment throughout the enterprise.

The Vision holds that there will be **a single, seamless network that delivers service to both the operational and support elements of the enterprise.** This implies that the network will be carrying a variety of traffic types, and will be attempting to optimize the results for each type of traffic. To accomplish this some form of Quality of Service (QoS) will be established in the network. QoS technologies provide the elemental building blocks that will be used for future business applications enabling complex networks to control and predictably service a variety of networked applications and traffic types. Currently there are a variety of competing QoS schemes being developed and implemented by various network equipment makers. It is the view, however, that within the next five years a standard will emerge with which all vendors will have to be compliant.

The Vision identifies that there will be a single, unified network to handle both administrative and operational functions. As a result the long-term technical design of the LAN must include a topology that does not allow for a single point of failure, and has an estimated mean-time-between-failures for aggregated core network components of greater than 99.99%. With this in mind the long-term LAN technical design incorporates multiple route selection and redundancy in the core backbone, and redundancy of all network elements. In short, there is neither a single point of failure, nor a single path in the core (vertical). The long-term technical design recommendation, however, does not include redundancy to the desktop (horizontal) as it would be cost prohibitive and would gain little for the organization.

Other areas for consideration in implementing LANs are Security and Network Management, which are described in Sections 8.6 and 8.7.

7.2 WAN

Many of the long-term technical design elements associated with the LAN portion are mirrored in the view of the WAN. Indeed, the Vision would dictate that they be viewed as one-in-the-same. Over the long term, even with advances in automation, Hydro will continue to operate significant facilities in remote locations. Given the diverse nature of Hydro's physical locations it is recommended and anticipated that the basic WAN topology currently in place will continue to be used on a go-forward basis.

In the future **this network will support all of Hydro's production and support functions, and as such must provide for the requisite availability and redundancy levels**. That is, it must provide no single point of failure and provide an estimated availability of 99.9%. Therefore the long-term technical design is to provide WAN connectivity to all Hydro branch sites with a backup connectivity option. While the backup connectivity option does not have to provide the same level of bandwidth as the core, it must be able to handle all the traffic designated as essential and time-critical under the QoS routing scheme developed for the network.

In the core of the Hydro WAN topology, the closure of rings is recommended. That is, the long-term WAN technical design is based on a series of closed rings implemented in such a fashion that a break in any one portion of the ring results in traffic automatically being routed back along the other side of the ring to its intended destination. This has become the standard topology for most WAN networks in place today.

Another consideration in developing the WAN view includes the issue of protocol selection (Layer 3), security and network management. Currently there are a variety of protocols in use within Hydro to carry both the voice and data traffic, as well as the SCADA information for the EMS network. Given the vision of a single, unified network a fundamental decision will be required on protocol selection in the core. The long-term WAN technical design incorporates an IP-based packet switched network for all traffic with appropriate QoS measures implemented to ensure priority routing can be provided to mission-critical data. This results in all applications moving to an IP-based approach under a fully managed network, including IP-based SCADA and Voice over IP. As traffic is migrated to IP, consideration must be given to the level of encryption required. WAN Security and Network Management are covered in Sections 8.6 and 8.7.

At a transport layer (Layer 2) there are also several options for protocols. After a review of possible options, including ATM, packet-over-sonnet and raw Ethernet, it is recommended that Hydro's long-term WAN technical design be based on a serialized TDM topology. This will provide Hydro with the most efficient use of the relatively expensive WAN connectivity infrastructure, while allowing it to "turn up" bandwidth as future applications demand. An overview of the recommended long-term technical design is shown in Figure 6.

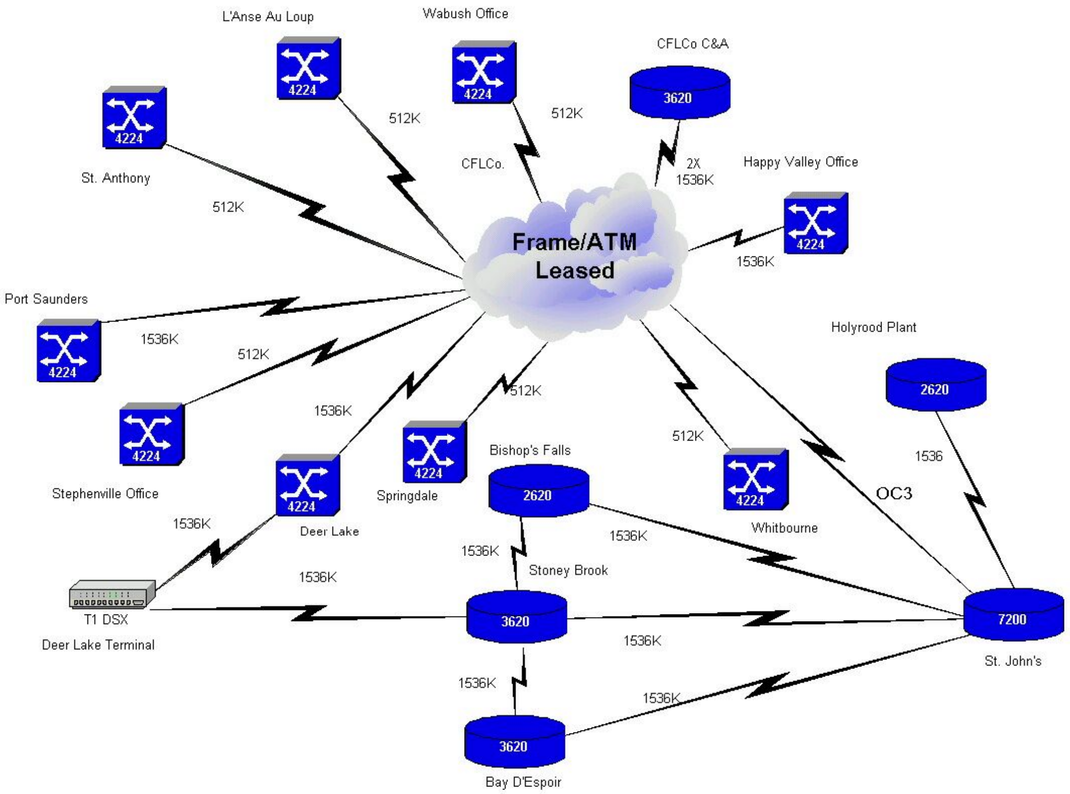
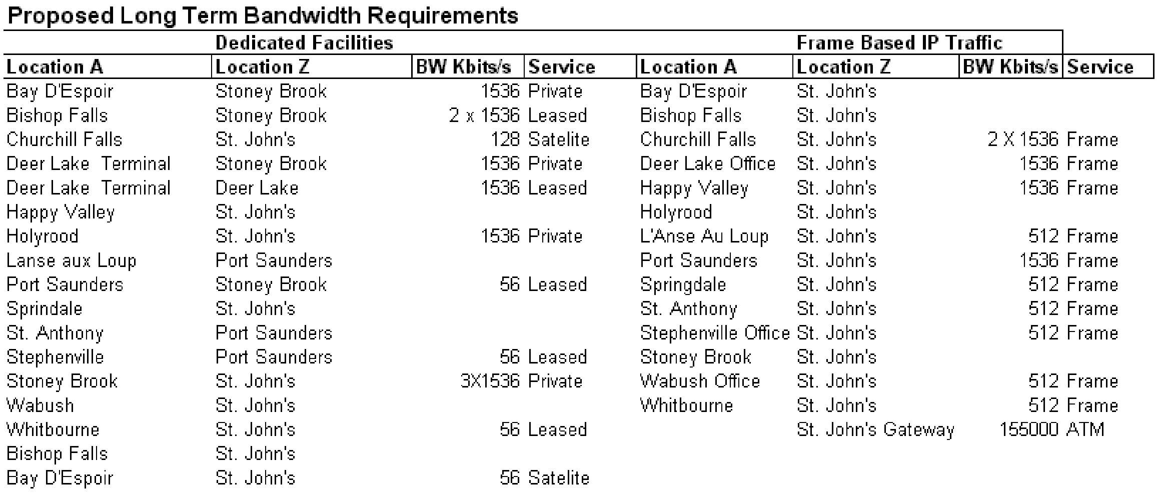


Figure 6 - Long Term WAN Technical Design

The long-term WAN topology was designed with the following strategy in mind:

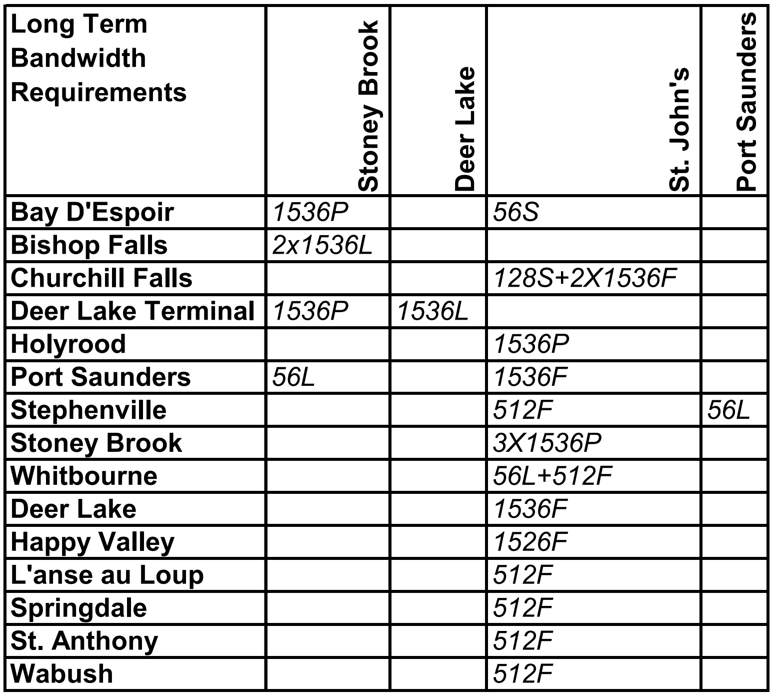
- Latency, jitter minimization
- Support of types of traffic
- High availability
- Maximum Utilization of Hydro existing and infrastructure
- Migration from the non-manageable products
- Minimize use of disparate systems

As part of the long-term WAN technical design it is recommended that Hydro migrate to fibre access at all sites to improve service & reliability. Fibre does not have the EMI noise and induction safety issues associated with the use of copper as an access medium. As well, fibre is treated with a little more reverence than copper and thus tends to see fewer failures.



Proposed Long Term Bandwidth Requirements

Dedicated Facilities				Frame Based IP Traffic			
Location A	Location Z	BW Kbits/s	Service	Location A	Location Z	BW Kbits/s	Service
Bay D'Espoir	Stoney Brook	1536	Private	Bay D'Espoir	St. John's		
Bishop Falls	Stoney Brook	2 x 1536	Leased	Bishop Falls	St. John's		
Churchill Falls	St. John's	128	Satelite	Churchill Falls	St. John's	2 X 1536	Frame
Deer Lake Terminal	Stoney Brook	1536	Private	Deer Lake Office	St. John's	1536	Frame
Deer Lake Terminal	Deer Lake	1536	Leased	Happy Valley	St. John's	1536	Frame
Happy Valley	St. John's			Holyrood	St. John's		
Holyrood	St. John's	1536	Private	L'Anse Au Loup	St. John's	512	Frame
Lanse aux Loup	Port Saunders			Port Saunders	St. John's	1536	Frame
Port Saunders	Stoney Brook	56	Leased	Springdale	St. John's	512	Frame
Sprindale	St. John's			St. Anthony	St. John's	512	Frame
St. Anthony	Port Saunders			Stephenville Office	St. John's	512	Frame
Stephenville	Port Saunders	56	Leased	Stoney Brook	St. John's		
Stoney Brook	St. John's	3X1536	Private	Wabush Office	St. John's	512	Frame
Wabush	St. John's			Whitbourne	St. John's	512	Frame
Whitbourne	St. John's	56	Leased		St. John's Gateway	155000	ATM
Bishop Falls	St. John's						
Bay D'Espoir	St. John's	56	Satelite				



Long Term Bandwidth Requirements	Stoney Brook	Deer Lake	St. John's	Port Saunders
Bay D'Espoir	1536P		56S	
Bishop Falls	2x1536L			
Churchill Falls			128S+2X1536F	
Deer Lake Terminal	1536P	1536L		
Holyrood			1536P	
Port Saunders	56L		1536F	
Stephenville			512F	56L
Stoney Brook			3X1536P	
Whitbourne			56L+512F	
Deer Lake			1536F	
Happy Valley			1526F	
L'anse au Loup			512F	
Springdale			512F	
St. Anthony			512F	
Wabush			512F	

Legend

Satellite	S
Frame Relay	F
Leased Dedicated	L
Private Dedicated	P

7.3 Internet

The Internet Access portion of the long-term technical design focuses on four aspects:

- Transport
- Access Points
- Caching / Proxy Server Configuration
- Secure Network Access over the Internet

It is proposed that Hydro have **a single, unified network for all applications**. As a result, all Internet traffic within the network would navigate the network under the same QoS scheme as other traffic. Currently administrative traffic and Internet traffic is segregated to eliminate the load impact Internet traffic would have on the administrative traffic.

Over the long-term, Internet access will become increasingly integrated into the operations of the company, to a point where inability to access the Internet will negatively impact business operations. With this in mind access to the Internet must be designed to avoid single points of failure in much the same way that the LAN and WAN are designed. As a result the long-term technical design for Internet access includes a second Internet access point that can be used for either load-balancing or strictly for backup. As part of this design the Hydro network would be configured with multiple routes to the Internet to minimize any downtime caused by an ISP losing connectivity.

In order to enhance the performance, as well as increase security, within the Internet portion of the Hydro network, the long-term technical design recommends the inclusion of both proxy and caching servers. The configuration would provide for no single point of failure. This translates into the strategic location of caching servers throughout the WAN to reduce the overall traffic and increase end-user response time. Placement of a proxy server in front of the Internet access to the two ISP's to proxy the traffic before leaving or entering the Hydro network is also recommended.

The long-term technical design **fully leverages the Internet as a remote access vehicle to allow employees to access their corporate resources from any location**. Under the design, secured access via the Internet will be provisioned to replace the current Remote Access Server (RAS) arrangement in place at Hydro. **The long-term technical design includes the use of IP-enabled handheld devices such as PocketPC's or Meter Reading devices coupled with secure network access via the Internet over wireless to E-enable the enterprise, as described in the Vision. In essence, the use of secure network access via Internet extends access to Hydro's network to anywhere Internet can be obtained, even if over wireless.**

The areas of Internet Security and Network Management are covered in Sections 8.6 and 8.7.

Figure7 shows a high-level view of the long-term technical design for Internet access.

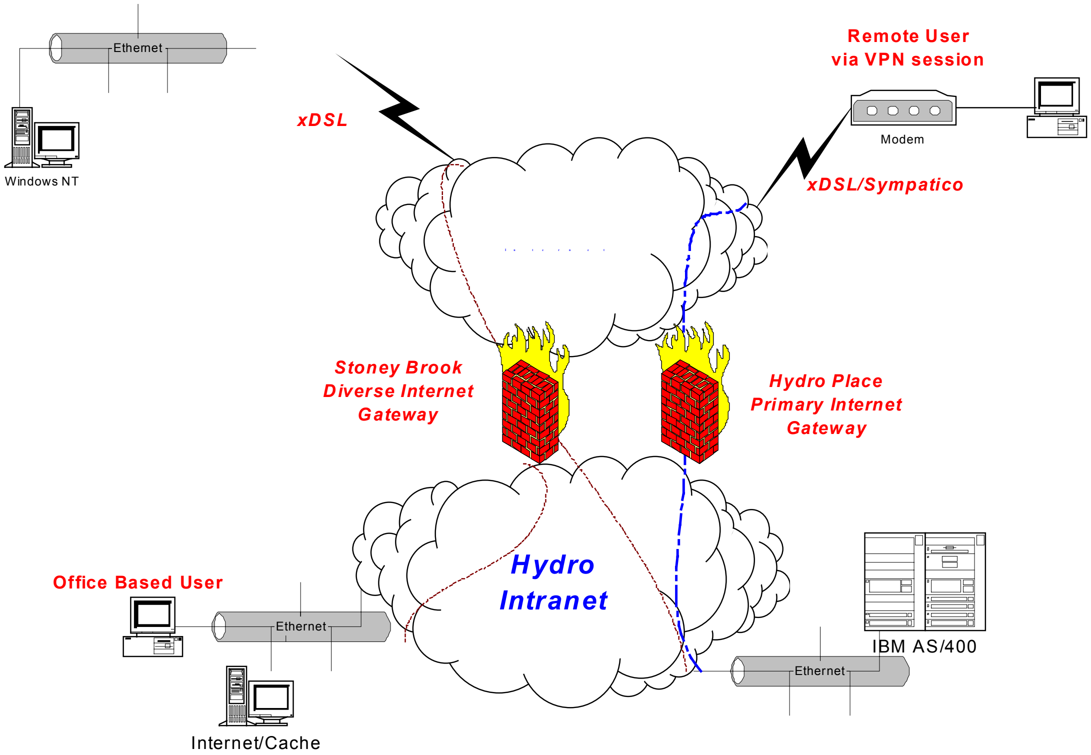


Figure 7 - Long Term Internet Technical Design

7.4 Core Applications / Processing Design

The Core Applications and Processing Design long-term technical designs are intrinsically coupled to each other and to the vision for the LAN/WAN infrastructure and Server Infrastructure. That is, there must be a coordinated view of where the organization is going so that each element support driving towards that goal. The long-term technical design for Core Applications focuses on three main areas:

- ERP System
- Communications
- Information Management

From a long-term view of the Core Applications and Processing Design functions it is viewed that **Hydro should continue with its implementation of an integrated suite of applications that allow the business to capture data once and manipulate that information in a coordinated manner through the system to its eventual end-state.** This centralized role is currently being provided by JD Edwards. While the software used over time may change, it is intrinsic to the long-term technical design that Hydro would employ some form of ERP system to centrally manage all operational and support functions for the organization. In fulfilling the Vision it is important to recognize that the ERP system must be both comprehensive and integrated, and that the business processes of the organization must act in a complementary and not competitive manner.

The second area of focus for the long-term technical design is the development of a single, integrated messaging system that would enable Hydro employees to communicate through a variety of means. This would include applications such as Voice over IP, e-mail, Instant Messaging, fax and voice mail. Over the long-term view **Hydro will provide communications services through a unified messaging platform so as to complement the E-enabled business processes of the company**.

The final focus area for core applications is in the realm of information management. Specifically, as time progresses the most important asset for Hydro is going to become information, whether that be information on production systems, information on inventory, or information on financial results. In addition, the demand for information is predicted to increase, while the accepted turn-around time for that information is going to decrease. As a result developing and implementing an Information Management strategy will be key for Hydro's success. The initial elements of this strategy will be a Data Warehouse application and a Document Management application, as detailed in the short-term technical design sections.

Security and management of core applications are important to maintaining a stable solution and are discussed in Sections 8.6 and 8.7.

7.5 Server Infrastructure

The **server infrastructure is responsible for hosting and maintaining service to the end-user client base**, and consists of both core application and network servers housed at Hydro Place, and file/print and messaging servers distributed throughout the WAN. There are four aspects of the server infrastructure addressed in the long-term technical design:

- Availability and redundancy
- Topology
- Configuration
- Physical Environment

Given the requirement for 99.99% availability for these services it is necessary to provide full redundancy and High Availability (HA) clustering configurations for all servers. As with other elements of the network, there must not be any single point of failure in the design. The type and level of HA and redundancy varies depending on the type of server infrastructure in question. For distributed file/print and messaging servers the long-term technical design includes the implementation of a small cluster environment in the location, with one functional server providing an HA cluster to the other. That is, the file/print server would back up the messaging server, and vice versa.

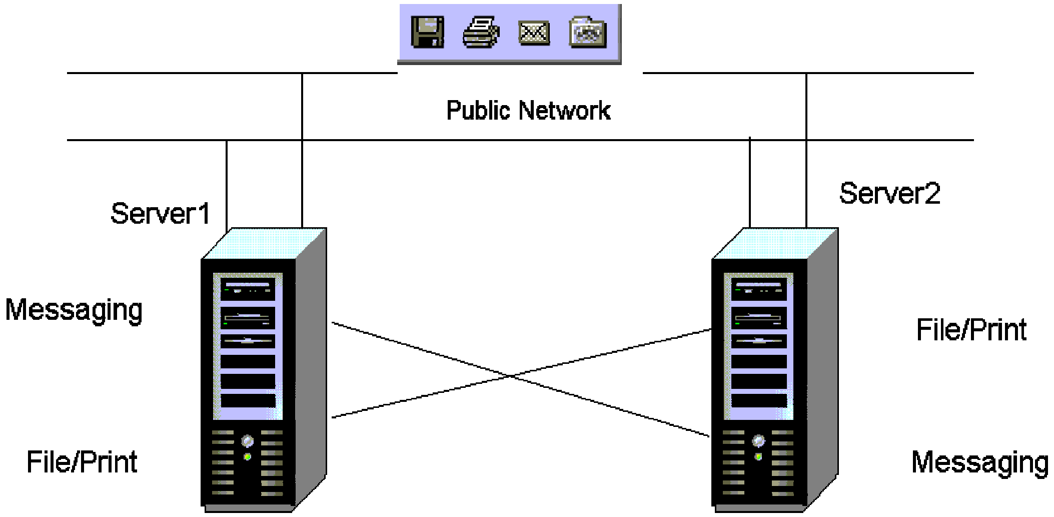


Figure 8 - Remote Office Server Configuration

For core network services the long-term technical design recommends creation of functional clusters. That is, servers that provide primary network functionality, such as DNS/WINS, Authentication, etc., would be provisioned in a functional cluster with a load-balancing switch in front.

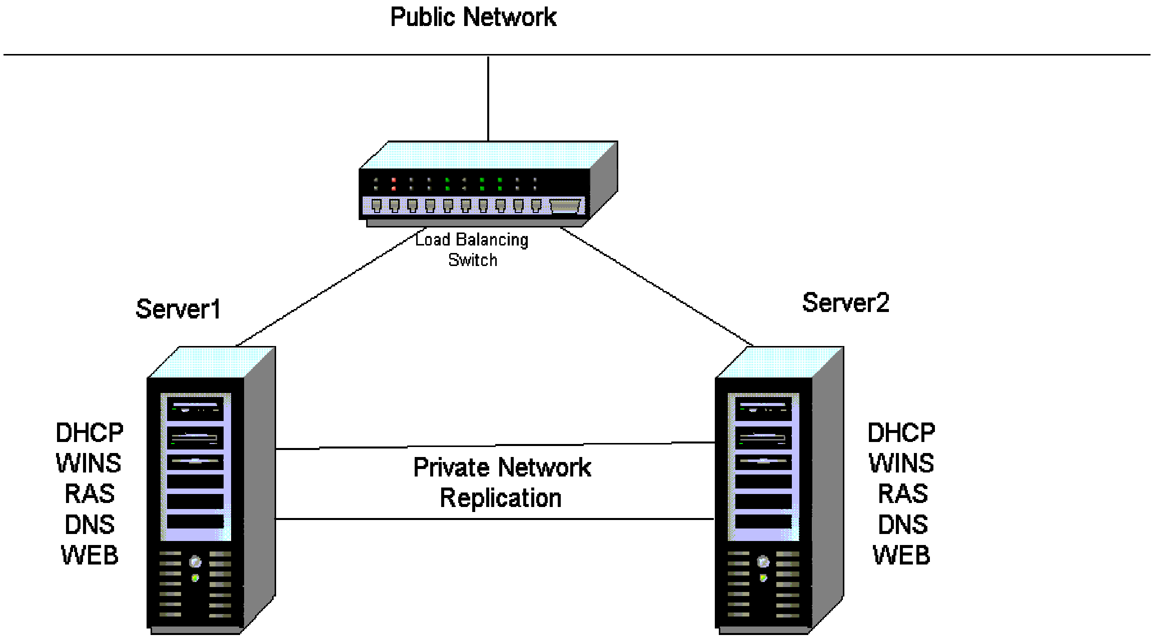


Figure 9 - Functional Cluster (Load Balancing)

Under this scenario there would be mirror images of the functional servers that would provide backup for each other in the event of a failure. Automatic failover would be achieved through the load-balancing switch configuration (also redundant) in that, if one server became unavailable, the entire load would switch to the available server.

The key factor impacting the sizing and deployment of the Core Application Servers is the application that they are hosting. Because an Applications Assessment was considered out of scope for this project, it was assumed that all current core applications would remain status quo. That is, there would not be a requirement to perform sizing on core applications servers unless there was a specified performance issue identified. Notwithstanding, two design elements are included in the long-term technical design of the core applications servers that must be incorporated for all applications. These are:

- A development and production environment configuration, and
- A Geo-HA production configuration

Because of the nature of the core application servers there are continual updates, patches and configuration changes that are being undertaken, which must not impact ongoing operation of the environment. In order to accomplish this there must be a combination of a development environment and a production environment in place. It is of critical importance that the development environment mirror the characteristics of the production environment so that testing on the development environment will ensure proper operation when moved into production. Similarly it is of vital importance that a proper Change Management and Staging process be implemented to ensure non-disruption of the production environment when changes are made. These processes are referenced further in Section 9.0 - Integrated IT Management Plan.

Due to the critical nature of the data located on the core applications servers, the long-term technical design recommends a Geo HA environment. That is, the servers would be in an HA configuration but physically distributed over moderate distance, with the heartbeat connection being established over dark fibre.

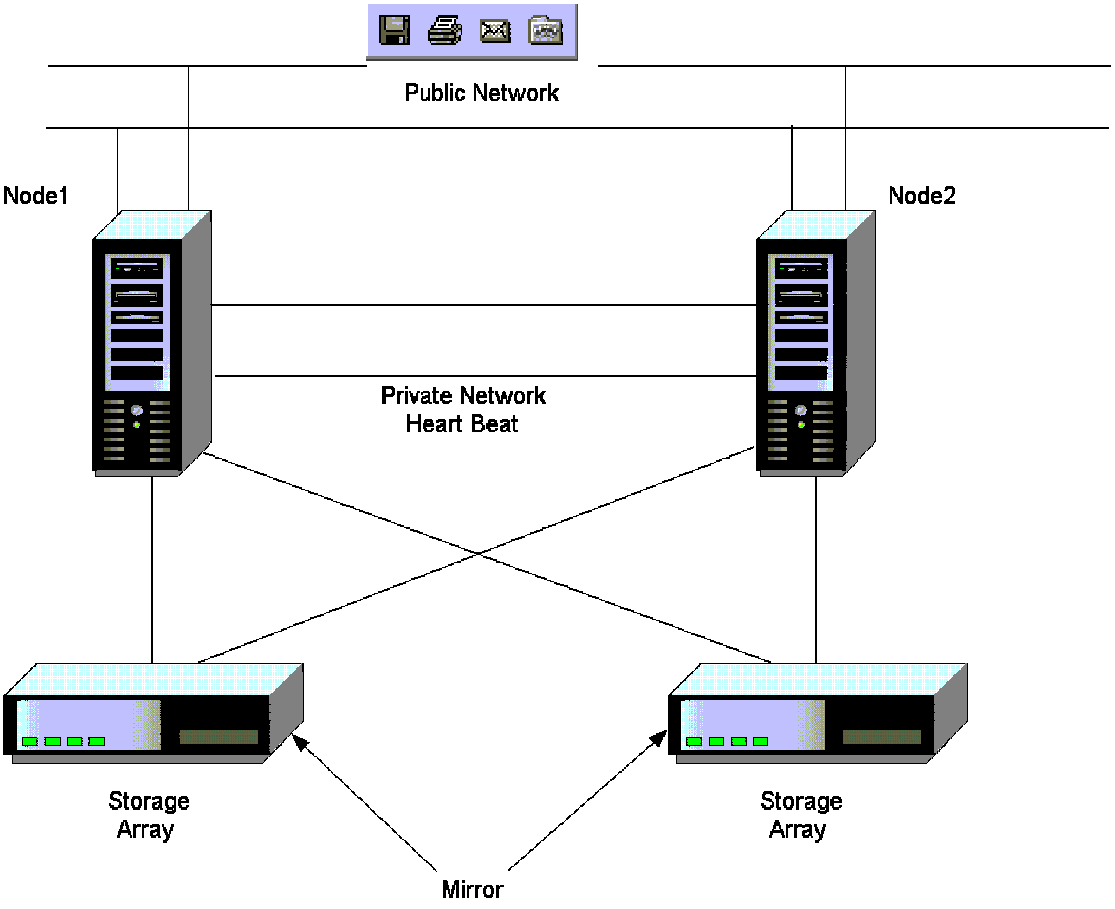


Figure 10 - Geographic High-Availability Cluster

In this scenario functions such as Lotus Notes, JD Edwards and the future Data Warehousing service would be clustered over distance with a Storage Area Network (SAN) in place to provide server-detached, processor-detached storage, backup and restore functions, as well as providing for Disaster Recovery planning.

From a topology perspective the server infrastructure will continue to be influenced by the WAN design over the long term in that the availability of WAN bandwidth will impact on the way in which services are distributed to the employee base. The long-term technical design for the server infrastructure includes reducing the overall installed base of server infrastructure in remote offices through use of a host-remote topology. Under this design a small office would act as a "remote" location of a larger regional office, which would house the server infrastructure. This would have the following results:

- Reduce the level of administration for the server infrastructure
- Reduce the investment in costly HA configurations
- Reduce the number of potential failure points in the network, increasing availability

Hydro has already started to use this approach in deploying its Lotus Notes servers and file/print servers. The trade-off for this savings, however, is an increase in WAN bandwidth demands at the edge of the network, where it is most costly to provision. It is believed, however, that the relative cost incurred by the slight increase in bandwidth demands (all core applications will continue to require WAN bandwidth back to Hydro Place) is more than offset by the cost savings in reducing the administrative burden and capital investment requirement. The resulting bandwidth requirements are included in the long-term WAN capacity reflected in Figure 6 Long Term WAN Technical Design and associated table.

The long-term technical design incorporates the extensive use of HA clustering technology to provide the required availability and redundancy in the network. With this in mind it is necessary to limit the types and configurations of servers deployed in the network to reduce potential conflicts in remote management as well as providing for economies of scale in sparing, service contracts, and technical training requirements. As a result the long-term technical design includes standardized configurations of tier-1 vendor equipment in the following classes:

- Remote File/Print and Messaging,
- Functional Clusters

The core application servers will continue to be based on stand-alone configurations, as dictated by the application requirements. As part of the standardized configuration there would be a centrally controlled automated backup system that would eliminate end-user process issues in performing backups. For the remote file/print and messaging servers the data would be stored off-site in the remote location, while for the functional clusters and core applications servers the data would be automatically backed up as part of the SAN environment.

Given the importance of the server infrastructure to the ongoing operation of the enterprise, it is of paramount importance that the equipment is provided with an appropriate operating environment to minimize controllable factors that may negatively impact the performance of the system. Given the capital investment required to provision HA clusters in the remote office locations, it would be prudent to provide for survivability of the equipment operation in the event of a power loss. With this in mind the long-term view is that all remote office server and communications equipment will be rack mounted in a dedicated (single-purpose) access-controlled space, and provided with a three-hour UPS power supply. This will allow for survivability of the network in the event of a power loss, instead of merely providing for a graceful shutdown of the equipment. In the Hydro Place location, UPS will be coordinated through a redundant UPS system designed to handle the power requirements for the data center for a three-hour period in the event of a power failure and diesel generator failure.

Management and Security considerations for servers are covered in Sections 8.6 and 8.7.

7.6 End-User Infrastructure

The final infrastructure piece in the long-term technical design is the end-user infrastructure. Specifically, **it is the way in which the end-users in the organization interact with both each other and the enterprise. As indicated in the Vision, employees will primarily use electronic methods to communicate within the enterprise, and with this in mind the long-term technical design has significant implications on the way people will complete their job functions in the future**. In developing the long-term technical design for the end-users consideration must be made of the future functionality to be delivered. Specifically, the differences in people's location and job function dictate different approaches to implementing end-user infrastructure. The Business Needs Research identified a variety of ways in which employees use the existing IT infrastructure. These can be classified as follows:

- **Support Staff** – Support staff are located primarily in Hydro place and provide staff functions such as HR, Finance, Engineering, etc. that are used by the production functions to manage and complete their tasks.

- **Production / Field Staff** – The production and field staff are located across the province and are involved in the daily production, transmission and distribution of power to Hydro's residential and commercial customer base.

These two general user groups dictate two different approaches to the long-term technical design for Hydro. For support staff much of the interaction with core applications will be dictated by the architecture for each application. The core applications will utilize a four-tier architecture whereby the end-user will interact with the system using a thin client arrangement. The specific thin-client architecture will be dictated by the location and function of the support staff. For those in support positions that do not require much local processing or specialized applications, the thin client architecture of choice is the use of an appliance device. Under this scenario a support person in a remote office would use an appliance with a smart card to work on JD Edwards, perform time entry, request reports or documents from the Data Warehouse, etc. For those support positions where a significant amount of end-user processing is required, such as conducting financial analysis, or where specialized applications are required, such as Computer Aided Design or Geographic Information Systems, a thin client arrangement using an application such as Citrix would be used. This would provide the end-user with a combination of local desktop processing power, as well as thin client access to the core applications. As with the server infrastructure, the desktop / laptop configurations would be based on standardized configurations.

The production staff and field staff have a different set of requirements. In order to allow them to interact with the system in the E-enabled environment described in the Vision, the production and field staff must have an access method. For those field staff located in vehicles or non-centralized locations, this is accomplished through the use of mobile devices and/or handheld devices securely connected to the company network over wireless IP. Under this scenario a lines person would have a handheld device that would use a secure connection over either a low bandwidth or high bandwidth connection to access work order information from the core applications. For production and field staff located in a centralized location, such as a production facility or warehouse, access to the network resources would be obtained through the use of centrally located thin client terminals with smart card readers. Under this scenario multiple workers in a production environment would receive and update work orders, enter time on a project, etc. using an appliance terminal located on the production floor.

Management and Security considerations for end-user infrastructure are covered in Sections 8.6 and 8.7.

7.7 Security

As Hydro moves towards the vision of **a single, unified network the emphasis on security will need to increase**. In the past, if a virus impacted the messaging system the effects were limited to the administrative systems. **In the new environment, a virus infecting the network would have the potential to impact both administrative and production networks.** As a result, the application of security procedures will become increasing important, and as such security will become a pervasive design element. **Security is not a single piece of equipment or activity, but instead it is a combination of technology coupled with appropriate policies, procedures and culture to create a secure environment.** With this in mind the long-term technical design for security involves four elements:

- Development of Security Policy
- Standardized Configurations
- Centralized Protection
- Positive Identification

The foundational element of the long-term design is the development and implementation of a comprehensive security policy. This would also result in creation of associated supporting software/operating system configuration documents that would be controlled by a Security Policy Committee, designed to coordinate the security efforts of Hydro. The Security Policy Committee would act as the central authority in all aspects of physical and electronic security.

Generally accepted industry standards for security now include establishing a standard workstation configuration that is both secure and locked to ensure that users cannot make modifications. It is recommended that standardized configurations for both servers and end-user equipment be implemented, with appropriate steps taken to ensure alteration of the baseline configuration cannot occur without intervention from the helpdesk. This will prevent employees from altering the configuration, and potentially introducing viruses or other threats into the network from within. A secondary benefit from a controlled server and workstation configuration is reduction in future support costs.

xwave recognizes that some employees may resist the plan to lock down the configuration of their personal computer. The key to successful implementation of this policy change is effectively communicating to all employees the reasons for this change, and ensuring that the helpdesk support team can be responsive to changes and additions required on the workstations.

One security threat facing Hydro comes from attacks on the network initiated from outside the enterprise using methods such as e-mail viruses. In order to protect the organization from such attacks the long-term design for security recommends creation of a centralized virus protection system to scan internal user machines as well as incoming traffic, such as e-mail. Another element of centralized protection is the implementation of an Active Intrusion Detection system designed to proactively monitor activity both within and outside the network for signs of subversive activity. An Active Intrusion Detection system is further discussed in Section 8.6.14.

Another element of the long-term technical design is the development of a strong, positive identification for all network access. This would mean moving beyond the basic static Username and Password scheme currently in place to one where a verifiable positive identification of the end-user can be made. This would be accomplished through the use of a combination of digital certificates and the use of selected biometrics. This positive identification approach, coupled with dynamic VLAN's and the centralized data repository described in the Vision would allow Hydro to customize the end-user experience and provide an appropriate level of security for Hydro's production and administrative environments.

7.8 Network Management

The final element of the long-term technical design is Network Management. Specifically this refers to the ability to view the health and performance of all elements of the infrastructure (LAN, WAN, Servers, Applications, etc.) in real time, and to perform preventative maintenance and troubleshooting from a centralized location. This would be provided by a series of tools consolidated into a Network Operations Centre (NOC).

A Network Operations Centre is the physical nerve Centre of a heterogeneously dispersed IT infrastructure. It includes equipment and personnel whose function it is to keep Hydro's mission critical infrastructure running smoothly. It is comprised of a team of network and operational support specialists who monitor and provide troubleshooting services 24 hours a day, 365 days a year.

Constructing a Network Operations Centre is a difficult task, demanding that a wide range of technologies be employed in an integrated manner to monitor and manage a large, geographically dispersed network from a services perspective. As the nerve Centre of the service management model, downtime of the NOC must be minimized, which means the NOC must be built to the exacting standards of a datacentre with environmental and security services providing maximum uptime and fault tolerance (i.e.: HVAC, UPS, diesel, security, High Availability servers, etc.)

One of the key attributes of a successful NOC implementation is the integration between the toolsets employed in the NOC and those used by the other functional groups within Hydro.

Figure 11 below outlines some of the functions that must be considered when attempting to define the role of the NOC in the organization in a Service Management model.

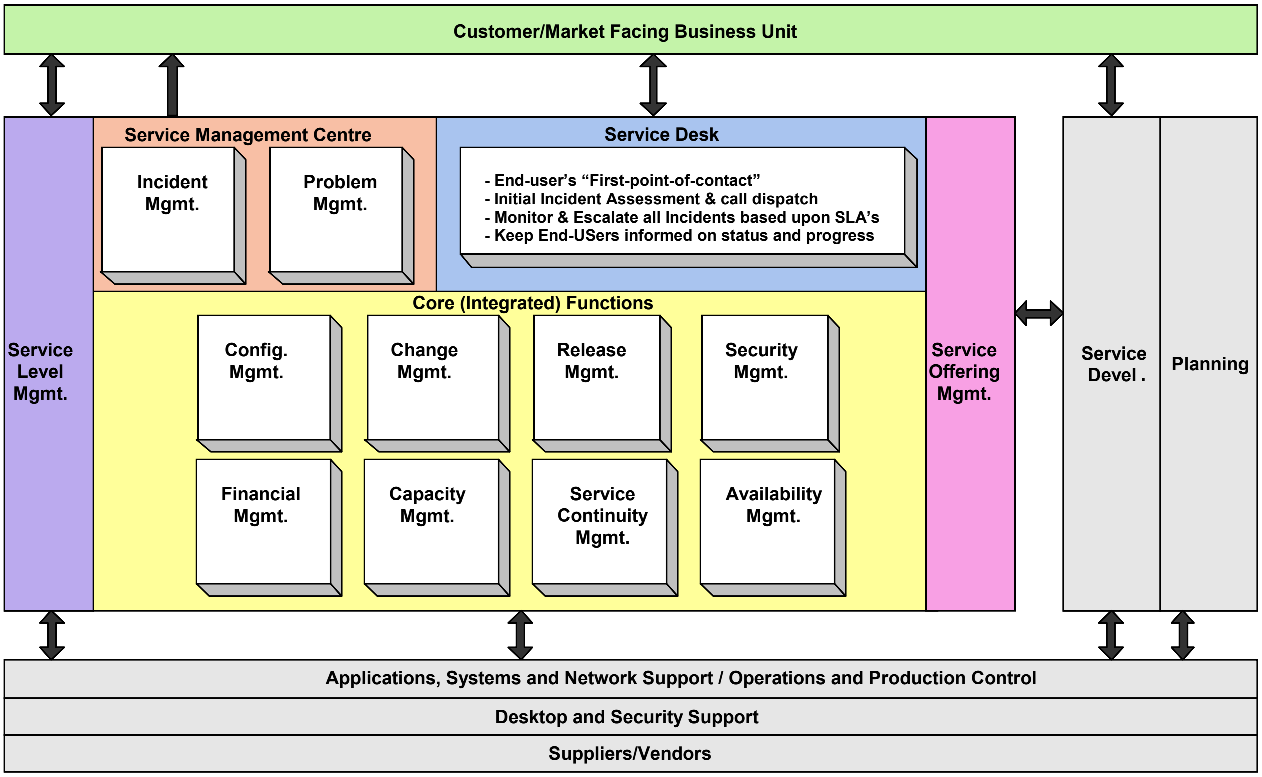

Customer/Market Facing Business Unit
Service Level Mgmt.
Service Management Centre
Incident Mgmt.
Problem Mgmt.
Service Desk
- End-user's "First-point-of-contact"
- Initial Incident Assessment & call dispatch
- Monitor & Escalate all Incidents based upon SLA's
- Keep End-USers informed on status and progress
Core (Integrated) Functions
Config. Mgmt.
Change Mgmt.
Release Mgmt.
Security Mgmt.
Financial Mgmt.
Capacity Mgmt.
Service Continuity Mgmt.
Availability Mgmt.
Service Offering Mgmt.
Service Devel .
Planning
Applications, Systems and Network Support / Operations and Production Control
Desktop and Security Support
Suppliers/Vendors

Figure 11 - Network Operations Centre Service Elements

The Hydro NOC should operate on a 24/7/365 basis. The NOC should be comprised of a single, centralized, high availability configured location. If deemed necessary, an alternate test/development/DR NOC could be established in another location. With this in mind the core NOC operations staff should be physically located together at the central site.

It is important at this point to differentiate between the NOC and the Service Desk (Helpdesk). The current Helpdesk function for Hydro operates on a business-hours basis and provides telephone and selected on-site support for end-users of the infrastructure. It is a reaction-based entity that is not involved in the proactive development of the IT infrastructure. Under the NOC concept there will continue to be a Helpdesk function (as noted under Service Desk in Figure 11), but it will act as only one potential point of entry for information into the NOC. Other inputs that will trigger actions will be received from other sources, such as an alarm from a monitored device, a SLA report , a Change Management request, etc.

The following is a summary of the responsibilities of the NOC as they relate to the components of the Information Technology Infrastructure Library (ITIL) Service Management model:

Service Support

1. **Incident Management** - "Restore normal service operation as quickly as possible with minimal disruption to the business".
2. **Problem Management** – "Minimize adverse effect on the business by errors in the infrastructure and, therefore, proactively prevent the occurrence of Incidents".
3. **Configuration Management** – "Identify, control, maintain and verify versions of all configuration items in the managed environment".
4. **Change Management** – "Ensure standardized methods and procedures are used for all changes to minimize the impact of any related Incidents upon service".
5. **Release Management** – "Ensure that all aspects of a Release [technical & non-technical] are considered together".

Service Delivery

1. **Service Level Management** – "To maintain and gradually improve business aligned IT service quality through a constant cycle of agreeing, monitoring, reporting and reviewing IT service achievements and through instigating actions to eradicate unacceptable levels of service".
2. **Financial Management** - "To provide cost effective stewardship of the IT assets and the financial resources used in providing IT services.".
3. **Capacity Management** - "Ensure that IT processing and storage capacity provision match the evolving demands of the business in a cost effective and timely manner".
4. **Service Continuity (DR) Management** - "Ensure that required IT technical and services facilities can be recovered within required and agreed upon business time scales".
    - **Availability Management** - "Optimize the capability of the IT infrastructure and supporting organization to deliver a cost effective and sustained level of availability that enables the business to fully satisfy its objectives".

Security

In an interconnected environment such as an enterprise network there are many types of data belonging to many different clients. Hence security is very important. All points of IT infrastructure and physical building infrastructure security are monitored throughout the NOC that is responsible for the escalation of Security alarms. They notify the proper people and following the proper escalation processes. It is important to note that the NOC would not be responsible for security policy.

Interfaces

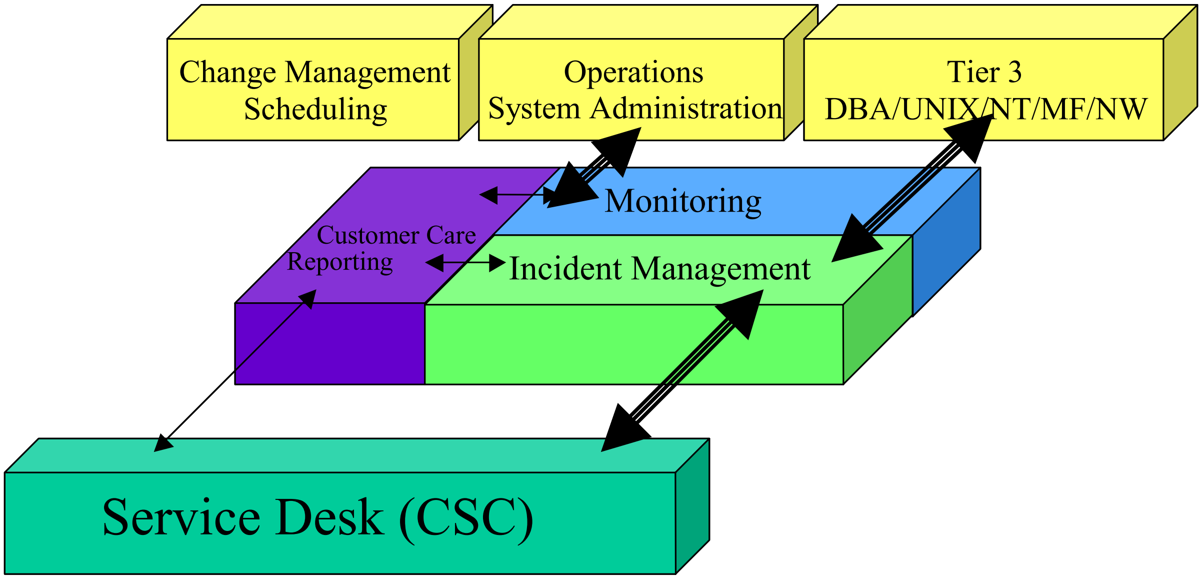


Figure 12 - Network Operations Centre (NOC) Interfaces

Service Desk (formerly referred to as Help Desk)
As noted previously, the Service Desk works hand in hand with the NOC. It acts as the end-users' first point of contact for all trouble calls and as first tier incident management. Any calls received, but not resolved by the Service Desk, would be forwarded to the NOC to be assigned for resolution as appropriate. Similarly, if the NOC identifies an incident or potential incident through its proactive monitoring it will communicate with the Service Desk in order to ensure as many end-user calls are readily handled without further escalation. It is critical that the selected Service Desk and Enterprise Console tools be fully (bi-directional) interoperable. The importance of the Service Desk to the successful implementation of Hydro's centralized NOC function cannot be understated since, at the end of the day, it is the function that interfaces directly with the end-users of the infrastructure.

Change Management and Scheduling
The NOC would coordinate unscheduled emergency changes and changes that have been approved by the formal Hydro Change Management process to ensure the changes occur smoothly and that any faults resulting from the change are discovered and resolved rapidly.

Operational process scheduling would similarly be monitored by the NOC to ensure all processes occur as expected and to resolve any error that may occur during a scheduled process.

Operations and Systems Administration
IS & T staff are responsible for on-the-ground work in each Hydro location. This may range from backup tape swapping for NT servers to troubleshooting end-user issues in a Hydro

office. Similarly, the operations staff would be called on to perform routine maintenance such as clearing of temporary files to free disk space or installation of new hardware. The daily task list for the operators would be comprised of both regularly scheduled tasks as well as proactive maintenance tasks scheduled by the NOC through its response to Incidents.

Tier 3 Support

Tier 3 support specialists would provide the final level of incident management for problems that cannot be resolved by tier 2 staff and/or for problems that require vendor assistance. Tier 3 personnel are on-call to provide top level support for the Tier 2 personnel. They would be the only people able to access vendor support resources. It is envisioned that the Tier 3 support people will be geographically dispersed in order to provide dispatch capabilities.

8.0 Short-Term Technical Design

The next level of granularity required is to move from the Long-Term Technical Design, which focuses on the 10-year vision of the infrastructure, to the Short-Term Technical Design, which focuses on the immediate to five-year view. The purpose of the short-term design is to bridge the gap from the current state assessment to the desired direction for the long-term view through the application of relevant technologies and processes. In viewing this next phase in the development of the overall plan for Hydro, it is imperative that the short-term design is coordinated with both the long-term design and vision portions of the document.

8.1 Core Applications / Processing Design

8.1.1 JD Edwards

The JD Edwards suite is both highly integrated and far-reaching in its impact on the company. The tightly integrated nature of the system has significant impact on the infrastructure topology. First, there is little opportunity to create a distributed processing system due to the high level of interaction and common database elements associated with JD Edwards

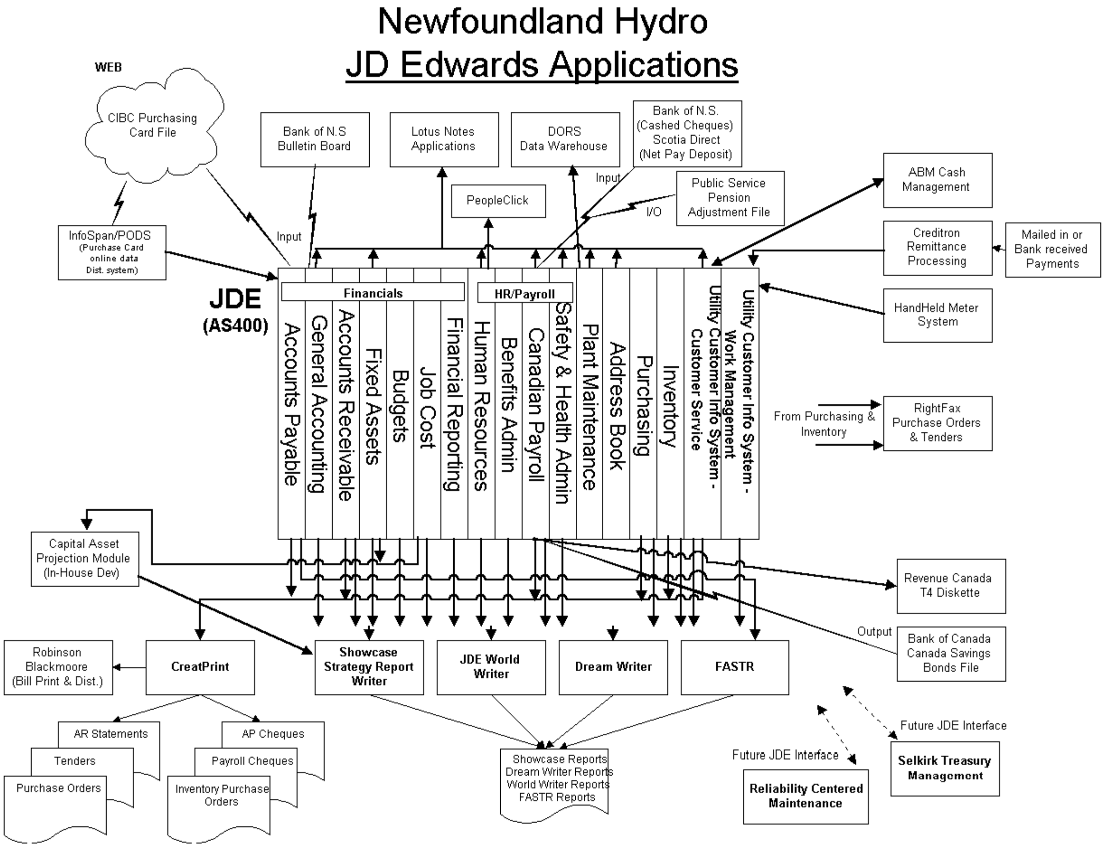

Newfoundland Hydro
JD Edwards Applications
WEB
CIBC Purchasing Card File
InfoSpan/PODS (Purchase Card online data Dist. system)
Input
Bank of N.S Bulletin Board
Lotus Notes Applications
DORS Data Warehouse
Bank of N.S. (Cashed Cheques) Scotia Direct (Net Pay Deposit)
PeopleClick
Input
Public Service Pension Adjustment File
I/O
ABM Cash Management
Creditron Remittance Processing
Mailed in or Bank received Payments
HandHeld Meter System
From Purchasing & Inventory
RightFax Purchase Orders & Tenders
JDE (AS400)
Financials
HR/Payroll
Accounts Payable
General Accounting
Accounts Receivable
Fixed Assets
Budgets
Job Cost
Financial Reporting
Human Resources
Benefits Admin
Canadian Payroll
Safety & Health Admin
Plant Maintenance
Address Book
Purchasing
Inventory
Customer Service
Utility Customer Info System -
Work Management
Utility Customer Info System -
Capital Asset Projection Module (In-House Dev)
Revenue Canada T4 Diskette
Output
Bank of Canada Canada Savings Bonds File
Robinson Blackmoore (Bill Print & Dist.)
CreatPrint
Showcase Strategy Report Writer
JDE World Writer
Dream Writer
FASTR
AR Statements
Tenders
Purchase Orders
AP Cheques
Payroll Cheques
Inventory Purchase Orders
Showcase Reports
Dream Writer Reports
World Writer Reports
FASTR Reports
Future JDE Interface
Reliability Centered Maintenance
Future JDE Interface
Selkirk Treasury Management

Figure 13 – JD Edwards Applications

processing. As well, due to the centralized nature of the application suite, the implied LAN and WAN network requirements reflect the need for some form of thin-client architecture.

Specifically, even java-based client interaction with the system would create significant traffic overhead on the network, resulting in potential congestion issues. It would be best if any interaction between the JD Edwards system and the end-client could be centralized in the Hydro Place data center, and the network be used as an “extension” of the keyboard, mouse and monitor through the use of Citrix in a three-tier architecture in the short-term, with an eventual move to a thin-client appliance model.

A second observation concerns the high level of interaction between the JD Edwards system and the various report-writing functions. Almost every module provides some level of output to a report writer. Standardization on a consolidated report writing function would reduce the number of potential interface issues that would result from system modifications. As well, in order to reduce the load placed on the network for providing reports, a standardized set of reports should be pushed through the network using the Lotus Notes Databases in off-peak hours to provide more localized data closer to the end users.

8.1.2 JD Edwards World Vision

The JD Edwards World product in conjunction with World Vision has been on the market for a number of years. It is a very solid product but is dated by today’s standards in terms of application flexibility, interoperability and development tools. The World product by today’s standards is a closed computing environment based on a dated development language (RPG) and closed development tools. The client connectivity is a terminal based session without the benefits provided by windows-based applications including user configurability. The Vision product is an overlay to the terminal session giving the appearance that the application is a windows-based GUI application. This provides only limited configurability which requires central administration for all changes. This application is not open-standards based and is limited in the functionality it can deliver to the client.

One World is the client server version of JD Edwards ERP software. It offers many advantages over the World product in the areas of flexibility, scalability and configurability. The One World application is interoperable with open based tools such as Visual Basic. The client component offers the advantages of most windows based applications such as online help, consistent with windows look and feel and interfaces with common office automation application such as Excel, and Word. Although JD Edwards still supports the World product their focus is now directed to the One World product suite. Another important note is that as of the next release of OneWorld, named B9, coexistence with World will no longer be supported. JD Edwards will continue to retrofit most of the go forward functionality into the current OneWorld release called Xe.

Based on the evolution of client server computing and the information provided above, our recommendation is that Hydro start the process of preparing for and implementing One World in a coexistent environment for development as soon as possible. The gaps identified in the above section should be reviewed further and a go forward plan should be put in place to address those gaps by priority to insure the infrastructure is positioned correctly to receive OneWorld when required. Although JD Edwards will continue to maintain a compatible OneWorld release for coexistent implementations the concern is that they will also focus most of their efforts on the newer more mainstream versions of OneWorld. The second concern is that these versions will not take advantage of newer functionality as quickly as the mainstream versions.

8.1.3 Lotus Notes

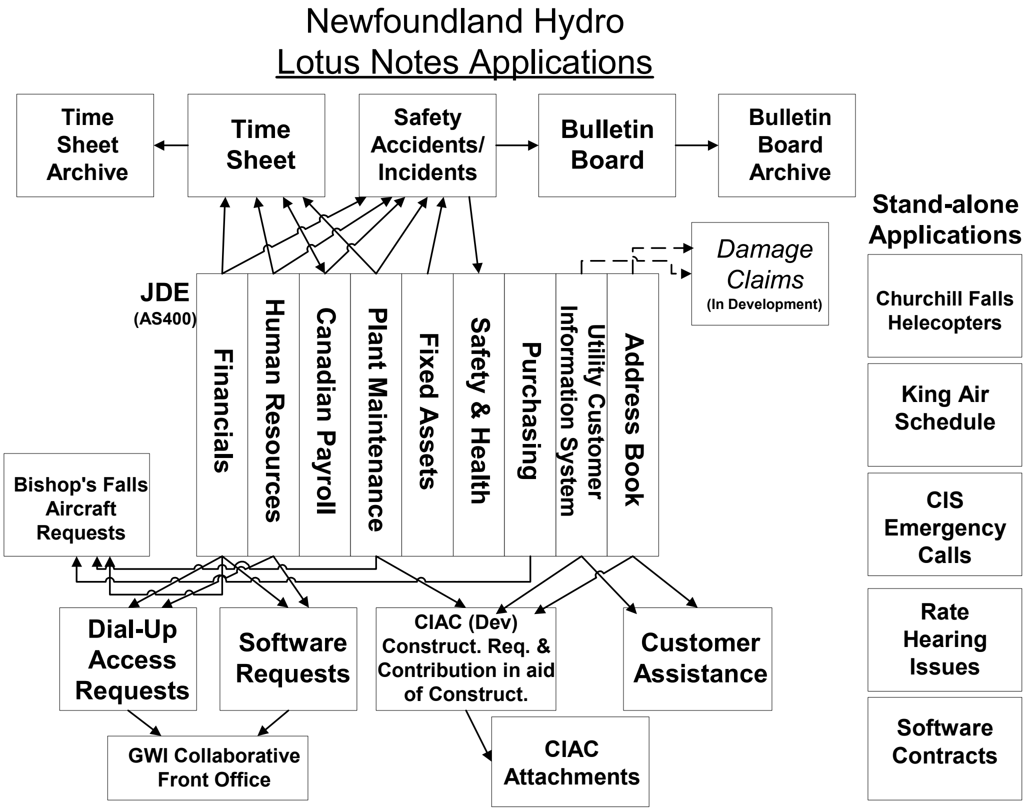


Figure 14 - Lotus Notes Applications

There is a significant level of interaction between both the Time Sheet application and the Safety Accidents / Incidents application and JD Edwards. Due to the pervasiveness of the Time Sheet application and the significant number of reported latency issues, a further investigation was conducted.

The Time Entry application is a Notes database that allows users to enter their time each day. This database also contains workflow to allow for the approval of previously entered time. This mission critical application is highly utilized within the organization and several inefficiencies have been indicated. Due to architecture design of the application it makes several calls to both the local notes server and the AS400 located at Hydro place; which reside in St. Johns, NF. This architecture presents significant inefficiencies including unnecessary network traffic and slow processing time during the processing of time entry.

Four areas that should be further analyzed to aid in increased efficiency are:

- Dual validation of data.
- Calls to servers located off site
- Improper scheduling of replication
- Unnecessary and/or improper timing of scheduled agents

Note: Although system analysis was only done on the Time Entry System other applications developed in house use similar workflow and technology; therefore; the above observations may apply to a number of other Notes applications.

In the medium term, Lotus is currently beta testing a new release called Domino Rnext. This new version of Domino optimizes a new streaming replication feature to improve replication across all servers. Rnext makes it easier to incorporate data and stored procedures from relational databases and ERP systems into Domino applications.

The new features in Domino Rnext build on the features in Release 5 to address rapidly changing industry trends. Lotus has combined both evolution and innovation in its latest upgrade of Domino server technology to meet corporate challenges head on.

8.1.4 Harris Energy Management System

A review of the Harris Energy Management system from an application perspective was outside the scope of this project. Notwithstanding, from an infrastructure perspective a number of short-term recommendations can be made. Specifically:

- Conduct knowledge transfer of how to support the Harris infrastructure to at least one additional Hydro employee since there is only one active support resource.
- Start immediately the process to replace the Harris EMS infrastructure. Experience has shown that it is a multi-year process.

8.1.5 Additional Applications

In addition to the existing core applications in the short-term view, several additional applications are required in order to meet the current business requirements of Hydro. The most pressing of these include a Data Warehousing environment and a Document Management system. The data warehouse environment is required to allow Hydro to manage the ever-increasing information needs of its internal and external client base. The document management system would provide an integrated central repository of information that would allow for collection and centralized management / storage of documents for Hydro.
Both the Data Warehouse application and the Document Management system would reside on a core application cluster located in the Hydro Place data center.

8.2 LAN

8.2.1 LAN Switch Architecture Overview

As a result of the review of Hydro's technical infrastructure, **xwave** and Newtel have developed a LAN / WAN architecture designed to provide maximum availability and flexibility. The design was constructed with a view to meeting the long-term vision of Hydro, and provides a scalable solution for growing Hydro's network as future bandwidth requirements increase with the evolution of applications resident on the network.

With this in mind, there are four main types of switch configurations envisioned in the network:

1. Chassis-based switch – This would be the main switching environment residing in the Datacentre at Hydro place

2. Fixed configuration switch – Fixed configuration switches would be used at major office sites and at selected locations within wiring closets at Hydro Place

3. Network Edge switch – Network edge switched would be located closest to the end users in the Hydro Place, Churchill Falls and Bishop's Falls locations

4. Combination Switch / Router / Serial Interface – The final configuration would be a combination switch / router / serial interface device that would be located at small office locations. It would provide for both layer 3 switching, routing and serial interface (T1) to the wide are network. The switch criteria for this configuration would be the same as for the network edge switch.

8.2.2 DNS / DHCP

In order to increase availability it is recommended that Hydro create backup DHCP servers for all locations by reserving 10% of the scopes for use on a second DHCP server. The backup server should be located at the other end of a WAN connection and the local router interface configured with a helper address to forward DHCP broadcasts to it. The backup DHCP server will have a scope configured with the reserved 10% address space, and will respond to DHCP requests if the local DHCP server is down. It is also recommended that DHCP helper addresses be added to routers in all locations without a local server. The nearest DHCP server must have a scope for the IP network at locations without servers. With this in place, a DHCP enabled laptop can be connected to any network and get an IP address without manual intervention.

In order to increase the reliability and availability of Hydro's DNS services it is recommended that Hydro implement an internal DNS that supports dynamic updates defined in RFC 2136. The dynamic updates from a DHCP server maintain "PTR" and "A" records at the DNS.

Second, Hydro should configure the Windows NT DNS service on all remote servers and have the local clients use this DNS for name resolution. The remote DNS's must be configured with forwarder addresses pointing to the DNS servers at Hydro Place so that DNS queries are processed there before going external. The remote DNS's will cache name resolution responses locally, decreasing name resolution traffic across the WAN.

Finally, it is recommended that Hydro make the internal DNS's at Hydro Place Primary and Secondary for the "nlh.nf.ca" domain by adding "SOA" records. This change will provide an internal DNS service for use across the Hydro LAN/WAN and allow access to hosts by name, not IP address. This will allow Hydro to change the IP addressing at the host with no change at the client.

8.2.3 Windows Evolution

Hydro has standardized on Windows NT 4.0 server single Domain model for its Intel based servers and NT 4.0 Workstation for the Intel desktops. This platform has served Hydro well over the last few years and the internal support staff is very comfortable with the current design. Microsoft and the reseller community seem positioned and committed to supporting NT 4.0 in the immediate future. All indications are that the move to Windows 2000 is a major undertaking and requires a major training and planning effort.

Windows 2000 service pack two and Active Directory is a maturing platform and a new Active Directory release is slated for 2002. This new release will address some of the limitations and problems with the current Active Directory. There are interoperability issues between the two Active Directory versions and implementing a mixed environment will be problematic, prompting early adopters to perform a second wide scale upgrade.

Windows 2000 and Active Directory is a major upgrade to NT 4.0 and requires extensive planning, testing and training. Current research indicates that the upgrade effort may be justified given the benefits of Active Directory and Windows 2000 but **xwave** suggests Hydro wait at a minimum until the 2nd release of Active Directory in 2002. When the next version of Active Directory is released, Hydro should revisit the option of implementing Windows 2000 and conduct a follow-up analysis. Should the upgrade be deemed a viable option, the first location for upgrade would be Hydro Place through an upgrade of the Primary Domain Controller, with subsequent upgrade and migration of the Backup Domain Controllers in the remote Hydro locations.

8.2.4 Backup Network

There has been a substantial increase in LAN bandwidth utilization in all locations during the nightly backups. This is caused when the server housing the tape backup unit pulls data across the network from other servers. As LAN activity increases, the backup window may extend into production hours in some locations and disrupt daytime LAN activity. This can be avoided by maintaining a separate backup LAN with connections to each server. Currently the only location that will benefit from a backup LAN is Hydro Place because of the high server count and distributed storage.

In the long term, the adoption of Storage Area Network (SAN) technology and server consolidation at Hydro Place will reduce the need for a separate backup network. SAN architecture can incorporate a backup device so data need not traverse the LAN and a busy LAN does not impede backup performance.

8.2.5 IPV6

The IRTF began work on IPv6 back in the early 1990's to solve IP addressing growth issues. Since then the adoption of CIDR (Classless InterDomain Routing) and NAT (Network Address Translation) has relieved pressure on the BGP routing tables and the IPv4 address space postponing the migration to IPv6. The IPv4 32-bit address provides four billion host addresses of which 40% are still unused.

The Internet started with end-to-end connectivity for any application but today NAT and application layer gateways are connecting disparate networks. The wide spread use of 'always on' devices such as Cable Modems, DSL, Mobile phones, gaming and residential voice over IP are promoting a return to globally accessible IP addressing.

The table below compares the features of IPv4 versus IPv6. Note there is little difference in the QOS and security features provided by IPv6 and the two, in fact, are interoperable.

IP service	IPv4 Solution	IPv6 Solution
Addressing range	32 bit, Network Address translation	128 bit, multiple scopes
Autoconfiguration	DHCP	Serverless re-configuration, DHCP
Security	IPsec	IPsec Mandated, works end-to-end
Mobility	Mobile IP	Mobile IP with direct routing
Quality of Service	Differentiated service, Integrated service	Differentiated service, Integrated service
IP Multicast	IGMP/PIM/Multicast/BGP	MLD/PIM/Multicast/BGP/Scope Identifier

To date, a limited number of organizations are testing IPv6 but it has not been widely tested or adopted. Hardware is currently not available to effectively support IPv6 on the WAN. Interoperability tools do exist, however, to facilitate connections to an IPv6 Domain if the need arises. For these reasons it is recommended Hydro maintain IPv4 for the short term 3-5 years and promote proactive application development by educating development staff in the ability to detect IPv6 addressing. It is recommended that potential IPv6 deployment be reviewed in another 3 years.

8.2.6 Physical Facilities

As was noted in the site visit assessments, locations for networking, telecommunications and LAN infrastructure in most locations were less than adequate. As a result, it is important that Hydro undertake, in the short-term, an initiative to develop appropriate facilities for this equipment. This is especially true as Hydro moves towards the long-term technical design, where integrity of the IT infrastructure is of paramount importance to the continued operation of the business.

8.2.7 Physical Wiring

As noted in the technical assessment there is a mixture of UTP category 3 cable, category 5 and 5e. The category 3 horizontal cabling must be replaced with category 5e or better and tested to support 100Mbit speeds. The vertical runs between data closets and the connection from the communications room to the computer room should be 6 pair multi-mode fiber tested at 1Gbit. The final destination for the fiber runs will be the core switch located in the Communications room on the second floor. This design will facilitate gigabit Ethernet connections from the core to the access layer devices and eventual migration to the long-term technical design of multi-gigabit connectivity in the core LAN backbone. It is also recommended that Hydro replace Token Ring equipment with SNMP manageable switches.

8.2.8 Core Switching

The current LAN at Hydro Place utilizes a collapsed Layer 2 backbone. **xwave** recommends a fully redundant chassis based Layer 3 core. Layer 3 switching at the core will offload inter VLAN routing from the 7206 and provide wire speed routing between VLANS. Redundant line cards are needed at the core to facilitate two load-balancing connections to each wiring closet. It is recommended that Hydro use two 16-port Gigabit Ethernet modules.

It is recommended that Hydro use a fully redundant single core switch. The alternative is to use a pair of smaller switches. The single chassis design model can utilize EtherChannel or Multi-link trunking, to grant redundant load balancing connections to the access layer, without the complexity of the Spanning Tree Protocol and load balancing VLANS.

Hot Standby Routing Protocol (HSRP Cisco) or Virtual Router Redundancy Protocol (VRRP ieee standard) provides a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end host. This protocol is designed to eliminate the single point of failure inherent in a static, default-routed environment. To enable this feature dual layer 3 routing blades are needed in the core switch.

For large offices outside Hydro place, **xwave** recommends a pair of layer three fixed configuration switches using Spanning Tree for fault recovery, and load-balancing VLANS to fully utilize bandwidth. Satellite locations and communications rooms should connect to the core via redundant Gigabit fiber connections.

For medium sized offices outside Hydro place, **xwave** recommends a pair of layer two switches using Spanning Tree for fault recovery. Redundant 100Mbps over Ethernet connections from any outlying buildings will provide a backup path if a core switch fails. 1Gbps connections to the core are not required because of low user counts. The servers and router require dual connections to provide complete redundancy.

For small offices outside Hydro place (25 users or less) it is cost prohibitive to install redundant core switching. **xwave** recommends layer three switches with integrated T1 WAN interfaces at these locations.

8.2.9 Access Layer

In line with the long-term technical design, the access layer at Hydro Place must be upgraded to a minimum standard of gigabit Ethernet in the core, and 100Mbit Ethernet in the horizontal layer. To accomplish this Hydro should replace all Token Ring devices with switched100Mbit Ethernet. The longer the two environments coexist the more difficult it will be for Hydro to move forward towards the long-term technical design.

8.2.9.1 IP addressing / VLAN

Logically separating the LAN into layer three VLANS will decrease the broadcast domain and increase security. Security is increased because access-lists can be applied to control inter-VLAN traffic. For the short term VLANS will be created based on location, in the future when dynamic VLANS are implemented new VLANS can be based on communities of interest.

The DHCP server will have a separate scope for each of these VLAN/IP subnets. It is recommended that Hydro utilize Dynamic VLAN technology to assign users to VLANS based on their NT username and password. It solves many of the day-to-day mobility problems within a LAN by ensuring that each user is appropriately associated with their authorized subnet/VLAN and that they all receive IP addresses that correspond to the logical groups to which they belong.

The technology must link to the network login process for dynamic registration of the user to the policy server and for control of user access to logical subnets and virtual LANs (VLANs). The user registration policy bindings should include login names, IP subnets, Dynamic Host Configuration Protocol (DHCP) addresses, Media Access Control (MAC) addresses, and user locations. User login information should intelligently monitor who the users are, the switch ports from which they are connecting, and the time of day they are accessing the network. After users are identified within the policy server, user tracking should reconfigure the switch ports on which they reside to the appropriate subnets, notify the policy server of these changes for tracking and auditing purposes, and reconfigures the Dynamic Host Configuration Protocol (DHCP) address of the workstation for IP address consistency. Further, it should provide active links between the user login process, DHCP addressing, and the switch port in which a user resides, and proactively communicate this information to the network management server for tracking and diagnosing problems with the network.

8.3 WAN

8.3.1 WAN Topology Design

An investigation of the WAN topology and infrastructure gave rise to a series of observations concerning the development and evolution of the WAN design at Hydro. Although the main processing center is Hydro Place, the IP crossroads for the company is actually in Stoney Brook though no traffic starts or terminates there. This design would appear to have evolved due the cost of bandwidth to each location and the dispersed Newfoundland geography that Hydro operations necessarily cover. With the completion of the digital radio system to St. John's, the constant reductions in bandwidth costs, and the need for high throughput, low latency, high availability routing the WAN design will have to consider how IP traffic is routed through the Stoney Brook site. Given that the demand for bandwidth is growing and the broadband radio network is due for completion in October 2003, constructing at least some T1 dedicated channels to the processing hub in St. John's may be warranted, rather than routing all traffic through the Stoney Brook router.

This design could eliminate the Stoney Brook router, however it would require a router in Deer Lake Terminal Station if a ring architecture were to be supported, as is envisioned in the long-term technical design.

8.3.1.1 Traffic Service Categories

The following points address the individual needs of each type of traffic area from a device & bandwidth optimization perspective and the potential difficulties of the integration of many media types.

- Priority 1 - SCADA – Low latency, low bandwidth, critical availability
- Priority 2- Time sensitive, non-critical, high bandwidth traffic (Voice & Video)
- Priority 3 - Real time application traffic 3-4 sec response on round trip query including intranet
- Priority 4- Internet traffic
- Priority 5 - Non real time traffic - sending mail, server back up, batch processing

8.3.1.2 Voice Topology

It is recommended that Hydro purchase an M1 PRI card for Holyrood and upgrade the PBX software as necessary to support digital services between Holyrood and ECC. Once completed this will allow Hydro to reduce the analog trunks to NewTel Communications DMS network in QIV 2001. As well, it is recommended that Hydro use a T1 from Holyrood to ECC for voice traffic that would bypass the GDC MUX and extends Calling Line ID to the site. There is existing hardware in the ECC and BDE voice nodes to support T1s. Therefore it is only a matter of turning up a dedicated T1 in Qtr IV 2001 when the radio system build is complete.

A second consideration concerns the construction of a digital trunk group off the DMS in Grand Falls to Stoney Brook with trunks running back to ECC and BDE. This would eliminate toll charge to Bishop Falls. The main advantage with this approach is the use of existing Hydro infrastructure and telephony features on stable toll-grade platforms for its voice network. The disadvantage is increased bandwidth consumption which may affect other applications during voice traffic lulls. In the long term this would be an issue, however in the next five years this should be acceptable as the bandwidth being constructed on the private radio network is more than sufficient.

In considering an immediate implementation of VoIP on the WAN it was concluded that it should not be implemented in the short term as it buys little bandwidth or cost savings. However, it does have significant implications from a LAN deployment perspective by the reduction of wiring and MAC effort. VoIP would also ease future integration of telephone functions with customer contact applications. It is recommended that Hydro start with a VoIP pilot project at selected Hydro place locations, with an eventual rollout on an attrition basis at ECC, BDE, BFL, HRD,CLF as soon as IP telephone equipment and operational costs drop and standards stabilize.

Finally, it is recommended that voice service be removed from TMS by either implementing VoIP or digital trunking. This will free up shelf space for other data services and ease migration from TMS in the long term. As a backup mechanism, cellular-based connectivity may be an option for VoIP telephone failures in selected sites.

8.3.1.3 SCADA

Supervisory, Control & Data Acquisition (SCADA) is one of the most important applications traversing Hydro’s telecommunications infrastructure. RTUs collect data from active power generation and transmission devices, which are then polled for state changes. If there is a state change, the Harris mainframe as the data reservoir requests the sequence of events (SOE) surrounding the state change. As well, grid control signals are propagated to their destination for grid management.

Ethernet attached IP based SCADA devices are quite attractive from an ease of deployment perspective and would support the long-term vision of Hydro’s network. For example, one switch could support IP SCADA devices, IP phone, site servers and PCs, etc. Unfortunately, the proprietary Harris protocol will have to be used until at least 2005 at which point Ethernet SCADA devices can be directly connected to the WAN if desired.

Operations

The SCADA traffic is deterministic and steady state type traffic, which means that the bandwidth will never be available for other applications. Thus it is immaterial from a bandwidth perspective whether or not it resides on the administrative WAN or on its own TDM circuit.

An IP network can meet the QoS needs of SCADA traffic through priority schemes as it only requires 1-2 second response time and jitter is not an issue as the data is all time-stamped at the source. In the short term Hydro should continue its investigation of IP/Ethernet attached RTUs that support RS232 interface in the interim but that are upgradeable during Harris retirement.

It is recommended that SCADA be moved to a separate IP based core network so that IP becomes WAN protocol standard and similar technologies (routers & switches) can be supported by the same skill sets and management tools. However, the WAN topologies should be *logically* separate. A completely survivable architecture would require two routers per site such that if the primary SCADA router failed, traffic could use the administrative router and network to reach its St. John's client. This would allow for router upgrades with only minor service interruptions

There are two types of traffic that are seen in a SCADA environment: historical data and graphs, and real time control commands and status queries. The historical/graphical component can reside on the administration network, however grid control traffic requires additional consideration. It is a low volume small packet type traffic that can be easily marked (known source & destination) to allow for prioritization, providing sub-second response times.

Realistically, even hardware that is capable of supporting 99.99% reliability doesn't eliminate the degree of complexity of the administration of this type of network and the high probability of highly dynamic traffic patterns causing periodic interruptions in SCADA traffic flows. Additional telecommunications circuitry may be a small price to pay for the ability to tune and manage the larger administrative network.

From a traffic volume perspective the testing preformed by Harris on the Ontario Hydro network revealed that during avalanche conditions in a 20-node site, traffic reached peaks of 20 percent on the LAN of which 50% traversed the WAN. This translates to potentially 1M on the WAN, a substantial volume, although Ontario Hydro's site may be somewhat larger than the typical substation that Hydro may be managing.

8.3.1.4 TMS Network

A TMS network is a proprietary GDC TDM (Time Division Multiplexor). It allows for the multiplexing of many different circuits types over the one facility such as SCADA, analog voice trunks and dedicated bandwidth for different applications. The network allocates bandwidth on a per circuit basis and has inherent inefficiencies. Though it does have the ability to reroute bandwidth and protect critical circuits in the event of primary route failures, it uses proprietary encoding which limits maintenance access.

TMS will be slowly phased out as more voice, data and SCADA devices become IP enabled, supporting a single, unified network topology. The Harris mainframe is the primary reason why this move can not take place in the short term.

8.3.2 Network Elements

Some routers do not support the 802.1Q standard. On a go-forward basis this may limit the ability of Hydro to implement QoS in the environment. All routers should be upgraded to a minimum standard of support for 802.1Q. Second, once a network management system is in place the maximum memory and CPU utilization per router should be assessed to understand where (if indeed at all) there needs to be additional capacity added to the network. Over the longer term the WAN routing infrastructure will carry increasing volumes of traffic and may pose a significant bottleneck if left unchecked.

8.3.3 Response Times

In reviewing the existing WAN configuration and response times there are several traffic optimization options that should be employed. First, traffic shaping to match the access speeds at either end of a frame relay based circuit should be employed to avoid congestion potential at the egress port, and thus help avoid retransmits. Second, the use of large access pipes (T1) over V.35 would minimize serialization delay. By purchasing serialized T1 bandwidth and constructing PVC's as required to match service demands, bandwidth can be increased incrementally; thus reducing both cost and network choke points.

Another option is to implement a single, larger frame relay circuit for both administrative and Internet traffic rather than separate facilities. This approach is both more attractive economically and will provide superior service. Sharing a larger frame port with either traffic shaping in place to cap the Internet bandwidth consumed, or a prioritization scheme in place to priority administration traffic during congestion periods is recommended. Initially when the larger frame relay port is established, traffic shaping would be applied to the network, as this would most closely emulate the current design. Prioritization schemes can then be implemented on a trail basis as required. It is important to note, however, that either a WAN bandwidth management platform or service be in place prior to attempting prioritization tests.

8.3.4 Short Term WAN Design Recommendations

8.3.4.1 WAN Design Criteria

The following is the criteria used as a boundary for the WAN design.

- Support for projected bandwidth
- Common Open Policy Services (COPS)
- QoS support across the WAN (layer 3) on all platforms
- Perform at 99.9% reliability
- Low Latency
- Scalable for future applications
- Multi-service support – Frame Relay, ATM, TDM
- Current network integration
- Maximize utilization existing infrastructure and skill sets

Detailed discussion of each item follows.

Application Bandwidth Demands

A complete discussion of application bandwidth demands is found in Section 8.8.3 – Benchmarking and Performance Metrics.

Common Open Policy Services

A Cisco QoS Policy Manager would allow Hydro to define rules-based policies that controls QoS application traffic across the network. The QoS Policy Manager can be used to set policies on devices that will control the bandwidth when there is bandwidth contention, otherwise data flow is uninhibited. QoS Policy Manager provides a network view of QoS policies deployed in the network and maintains an audit trail of all policy distributions.

- Centralized Policy Control
- Differentiated Service for Application Traffic
- QoS Domain Configuration
- Comprehensive QoS Feature Support
- Reliable Policy Deployment
- Web-Based Reporting
- Broad Device and IOS Release Support
- Resource Manager Essentials Integration

Traffic Flow and Traffic Management (QoS)

With new and more bandwidth hungry applications being introduced to Hydro's network there becomes the need to ensure that low priority traffic does not impairing the flow of mission critical applications. Introducing QoS architecture can minimize these impacts during short congestion situations. However, it should be noted that QoS must is not implemented as a means to replace bandwidth, as sufficient bandwidth must still be allocated to handle the day to day traffic needs of all the interactive users. Also, once in operation and effectively providing bandwidth to the higher priority applications the QoS scheduling algorithms will adversely effect the lower priority traffic.

Tools must be provided to assist in the management of introducing new applications and additional users onto the corporate network. The minimum to set would include a device monitoring/reporting/debug tool, a WAN bandwidth reporting tool and a policy server for QoS change implementation.

Traffic Shaping

Congestion & packet drops occur on the egress port of the Frame Relay switch if there is no traffic shaping applied at the router. This problem can be resolved by using traffic shaping on the router and move the point of congestion to the ingress router. Moving congestion from the Teleco Frame Relay switch to the router allows all of the above traffic prioritization methods to take place.

Traffic shaping in a Frame Relay environment takes place on each DLCI in the router. Traffic shaping applied to each DLCI creates congestion and the congestion effectively creates an output queue for each DLCI. This per DLCI output queue is called the traffic-shaping queue. An output queuing method is then applied such as the default FIFO or the CBWFQ. This traffic-shaping queue requires additional system buffer memory to accommodate the additional queuing. Another issue to keep in mind when using traffic shaping in network designs is to ensure that traffic entering the Frame Relay network from the router, on the ingress port of the Frame Relay switch, is never faster than the egress port of the Frame Relay Network.

8.3.4.2 WAN Reliability & Performance Calculations.

One of the design criteria was that the WAN have a reliability of 99.9% or better. A reliability analysis was completed on the topology and several critical and typical routes were analyzed.

Starting with MTBF (Mean Time Between Failure) statistics from the manufacture and MTTR (Mean Time to Repair) value of 4 hours. The statistical analysis showed a WAN Reliability Expectation exceeding the required 99.9% for all elements.

8.3.4.3 Latency

As part of the overall network latency evaluation two packet sizes were used during the calculation 68-byte (representing a typical VoIP size) and MTU of 1500 bytes.

The worst-case routes were used in the cases where there were redundant paths to a particular site. This would provide latency during primary route failure conditions. Where there were no redundant paths, the two worst-case routes were reviewed. Actual trunk measurements were used to determine propagation delay where available and mileage base estimations were use where not.

The calculations were completed based on substantial router load and are considered worst case. All sites fall within acceptable performance levels even during outage conditions. Acceptable performance was determined as a 68-byte packet traversing the WAN in less than 150ms in a single direction. Note that the sever turn around time must be added before a round trip calculation can be performed.

8.3.4.4 Short-Term WAN Topology

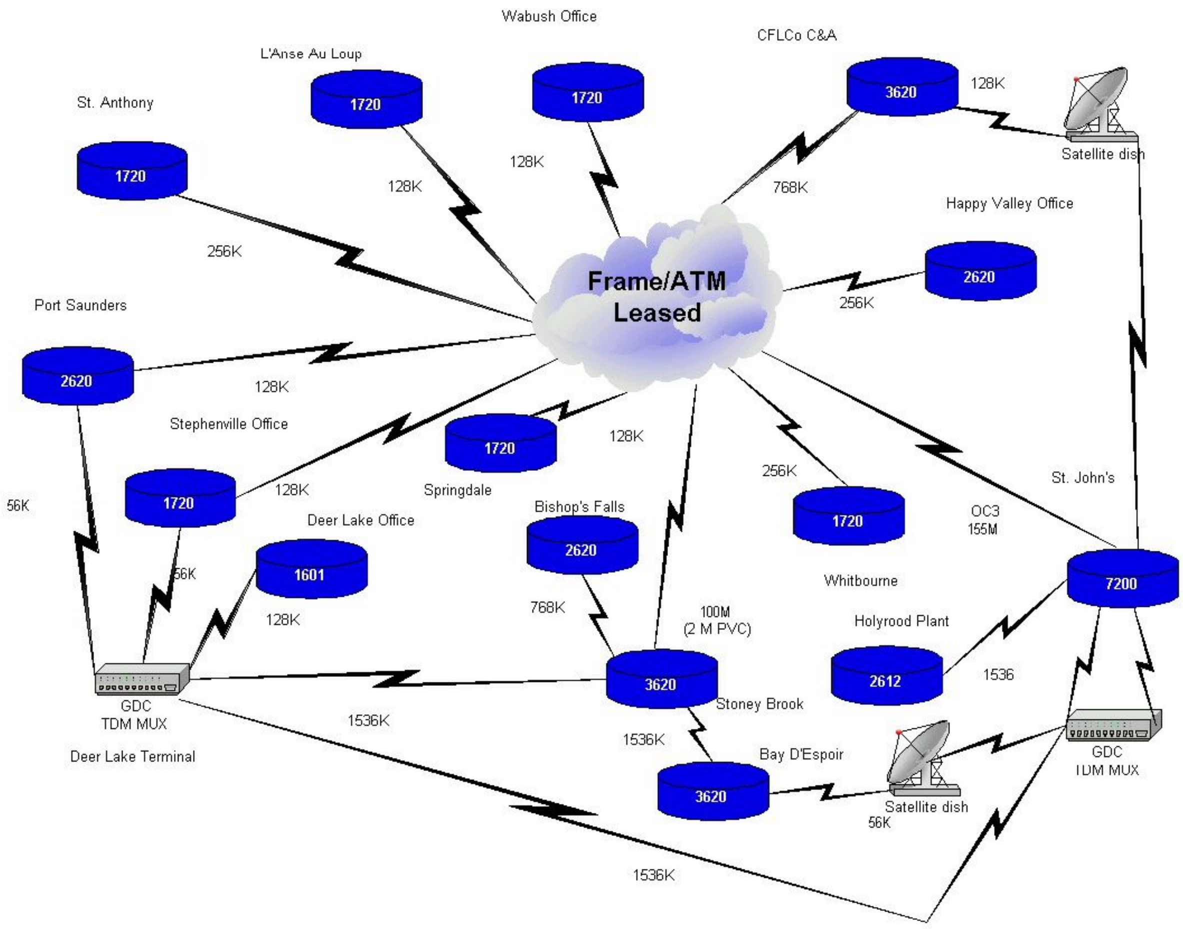


Figure 15 - Short Term WAN Topology

There are a number of short-term recommendations around the WAN design for Hydro's network. The first recommendation is to move the administrative network traffic to a frame-based network with the Internet bandwidth to take advantage of the economics of the frame, the OC3 ATM clocking to the 7206 and the latency improvements of single hop routing. This would result in increased bandwidth to all frame relay nodes to support both administrative and Internet traffic. To avoid issues with congestion caused by Internet traffic the available bandwidth to the Internet side would be capped using traffic shaping to ensure sufficient bandwidth remaining for administration traffic. This would require a decision on per user Internet service level to be provided to Hydro employees. In moving all traffic to a frame-based IP network Hydro would be able to remove all leased dedicated circuits except for the minimum required to support SCADA traffic.

A second recommendation concerns implementing an active WAN performance monitoring system.

A third recommendation is that Hydro deploy T1 cards in routers to reduce serialization delays. This provides the advantage of a 1.5M clock rate even though one may only be using a 512k circuit. As well, multiple services can be delivered down a single circuit to the router. As an alternative CSU/DSUs with an auxiliary drop and insert T1 port could be deployed at sites where both dedicated TDM SCADA DS0s and T1 based frame services are required.

Another short-term recommendation is to trial several QoS schemes on the frame service sites. This will allow users to take advantage of full bandwidth for their Internet needs when the admin traffic is low. This may not be required as in the very near future the Internet will be as important a tool as the administration application, which will slowly move to an http interface. When this happens prioritization will not be required. Having said this, the future WAN vision requires a QoS implementation to support the conflicting requirement of voice, multi-media, video and SCADA as they compete for space with the interactive data traffic and file transfers. Again one must consider the level of service that will be afforded the lowest priority traffic when selecting the size of lease facilities.

8.4 Internet

8.4.1 Internet Access Topology

Both the administration traffic and the Internet traffic should share a larger frame port with either traffic shaping in place to cap the Internet bandwidth consumed, or a prioritization scheme in place to priority administration traffic during congestion periods.

When many businesses initially connect to the Internet a primary concern is protecting their computer systems from the Internet. Another concern that frequently is overlooked is the potential for inappropriate activity on the Internet by employees. For this reason the generally accepted industry standard for connection to the Internet now includes:

- Establishing an Internet acceptable use policy
- Restricting network access to only the services that are approved
- Logging access by employees through various proxy-type services
- Reviewing the employee access and taking appropriate disciplinary measures

Vulnerability of IIS to attacks and viruses
A growing concern in the IT security arena is the protection of web sites from viruses and Internet worms. During the past year two major outbreaks of viruses directly attacked the security of Microsoft IIS systems (Code Red and Nimda). These viruses were spread through email and successfully disabled large numbers of IIS web servers throughout the Internet. These viruses took advantage of security weaknesses inherent in the IIS application software.

There has been extensive debate in the IT Security field whether the IIS software is secure enough for many businesses. All IIS systems that had added the latest security patch from Microsoft were not affected by either of these viruses. Many of the servers which did not have the patches applied were crashed by these viruses.

Enterprises such as Hydro that have deployed IIS for Internet facing web servers cannot easily migrate to a different software vendor. Microsoft has also promised to review the security issues related to their IIS product and release a new security enhanced version later this year. **xwave** recommends that Hydro greatly minimizes the risk associated with this software by following some basic security practices:

- Follow strict operating system hardening practices;
- Apply security patches to the operating system and IIS on a regular scheduled basis;
- Apply security patch updates on an emergency basis when an security alert is received;
- Ensure that all IIS servers connected to the Internet are properly protected behind a firewall;
- Perform regular vulnerability scanning on these systems;
- Implement a Host-based intrusion detection solution;
- Have an effective anti-virus protection program that includes:
    - Monitoring of detected viruses;
    - Regular updates to virus detection software;
    - Ensure regular reviews of the virus protection program.

8.4.2 Bandwidth Review

Aliant Telecom connected a network analyzer to Hydro's 10M Internet access to determine the grade of service being delivered by their ISP. The findings show that the 10Mbit Internet service current used by Hydro is not dedicated. It can be described as a half-duplex switched service with shared broadcast domain. Twenty-six (26) machines including other ISP customer's NT servers were identified to be sharing the segment with the Hydro. Foreign broadcast traffic was measured at one frame per second, which didn't have a significant impact on throughput.

The throughput for a FTP'd file was measured at around 800kbits per sec. This is a reasonable service level expectation for a half-duplex access.

8.4.2.1 Recommendations

IP multicast storm protection is recommended. An ISP with VLAN support should be explored to overcome this potential problem. The Internet service would be improved if it were delivered over a VLAN as this would increase security, eliminate broadcasts from other users on the segment, and reduce the risk of a broadcast storm causing service impairments. An upgrade of the access router to full-duplex 10baseT hardware will provide improved throughput when migrating to a VLAN topology.

Statements could be added to access router to eliminate the ARP requests, thereby providing minor throughput improvements to the Internet. Permanent static ARP entries will stop the router from re-ARPing once the entries are dropped from its table.

The enable password on the Internet gateway router should be removed, as it is easy to hack. The secret password will provide improved security.

A "no ip unreachable" statement should be added to the access router so that access list hits won't be broadcast to the shared domain. Type code 3 and destination unreachable replies will be shut down reducing the risk of outside parties discovering Hydro's network.

Changing the access list to have it applied to the outbound interface toward the PIXs will provide better protection. The router tends to miss 30% of packets on inbound lists during busy periods. Outbound lists catch almost 99%.

It is recommended that initially when the larger frame relay port is established that traffic shaping be applied to the network. This will most closely emulate the current design. The implementation of prioritization scheme will require network management tools or services so that congestion can be monitored. Traffic prioritization also requires corporate decisions on the weight to be placed on different types of traffic as these priorities would be constantly evolving as new services are added to the WAN. Other future traffic classes such as VoIP and Video will introduce the requirement for more complex prioritization schemes in the immediate future.

8.4.3 Single Point of Entry

The current single point Internet access has fewer security risks and less firewall management issues than a multiple Internet access topology.

The only region site outsides St. John’s that high-speed internet service can be delivered is Stoney Brook, and this site is a traffic hub with no clients on premises. If a broadband Internet service was installed at this site, the service would have to still be distributed over private and leased facilities to reach the end users. This option was considered, however, spare backup bandwidth between St. John’s and Stoney Brook was a more economic option. The approach of using a second Internet access only has merits if Hydro becomes dependant on the Internet from a day to day business perspective. At that point, the second access would provide service redundancy. While this is expected to be the case in the long-term, this recommendation is included as a long-term technical.

8.4.4 Internet Cache Application

It is recommended that an Internet cache application be deployed at each regional site so that frequently served up sites from both the intranet and the Internet can be delivered locally providing less strain on the WAN. In many cases, existing on-site servers can accommodate this functionality.

8.4.5 Remote Access Server (RAS)

Hydro currently has a RAS server at Hydro Place and dial in users call either an 800 number or local number to access the corporate network. If the employee only has a modem in his PC, and there is no other Internet connection to his PC, this is quite a secure solution. However, with the role out of high-speed Internet services, the potential exists for employees to be connected to the Internet on one port on their PC and the corporate network via dialup. This opens a small but possible security hole. It is recommended that Hydro construct a VPN network (leased or private) and provide employees who subscribe to high-speed Internet services access to the corporate network via VPN.

As part of the short-term technical design it is not recommended that VPN be deployed over dial-up Internet services, as encryption overhead will cause increased latency over an already slow dial connection.

8.5 Infrastructure

8.5.1.1 Servers

In reviewing the installed base of infrastructure for the Remote Office Cluster, it is evident that the File and Print servers were recently upgraded in most locations. The general specification is more than adequate for Hydro's general file and print needs. It has considerable scalability for additional RAM and disk capacity and depending on the initial configuration may be upgradeable to dual processors. In some cases Lotus Notes is also operating on the same server. This configuration tends to be restricted to very small offices and should not have any adverse affect on performance.

This dual-role server configuration does not, however, provide for the specified level of availability (99.99%) due to the lack of dual redundancy in the machines, and no clustering environment. As a result Hydro should move to implement clustering in the larger offices, with a view to an across-the-board roll out over the next five years in order to act on the long-term technical design.

Depending on the office size and number of people supported by the infrastructure it was possible there were additional file servers present. A plan should developed to out-service these machines over the next 36 months and migrate their applications to either a Remote Office Cluster or a Functional Cluster as defined in the long-term technical design.

The Functional server configurations are the primary focus of the LAN short-term design. As such, Section 8.2 of the report is the main vehicle for making recommendations concerning the functional server configuration.

The final configuration is the Core Application Cluster. As noted, the specifications on the Core Applications servers are primarily dependant on the results of an Application Assessment. During the course of the investigation there were no specific performance issues related to the server configuration for the Core Applications uncovered and as such the short-term design does not make any recommendations concerning changing or upgrading these servers. The primary recommendation is that all core application servers have a configuration that allows for clustering of the production application server (as is currently in place) and a development environment for testing changes and upgrades prior to staging to production.

8.5.1.2 Servers – High Availability / Redundancy

The current clustering arrangements are steps in the right direction for Hydro. The use of Microsoft Cluster for file/print and SQL servers and Microsoft Cluster with Domino Cluster for the Lotus Notes servers provides a good foundation for moving further into the HA clustering arena, as designated in the long-term technical design. In order to achieve the long-term vision, clustering must be implemented in the three areas of:

- Core Application Servers - Geo HA
- Functional Clusters
- Remote Office Clusters

Currently Hydro has implemented HA environments for some of its core applications servers, but none of its functional servers, such as DNS/WINS, DHCP, Authentication, etc., nor its Remote Office server environment. Selected implementations of these clusters must be initiated now to provide Hydro with the experience required to move toward the long-term technical design. As well, in order to achieve the 99.99% reliability required in the network, all network and application servers must be provisioned in an HA arrangement.

Within the existing server environment redundancy has been built into the server infrastructure in terms of disc space, CPUs, and RAID-5 technology. This level of redundancy is adequate as it eliminates the single-point of failure within the individual servers.

8.5.1.3 Data Center

The racking of server equipment should continue as it optimizes space in the data center environment. The use of a KVM switch for racked equipment is recommended as it reduces the overall capital expenditure and provides additional server space.

The datacentre is partially carpeted which increases the level of dust particles and increases the chances of static electricity interfering with the servers. In addition, carpeting makes it more difficult to get into certain areas underneath the raised floor.

In any electronics-enabled environment the presence of water in any form is not recommended. Though not recommended, one alternative to a wet-pipe system is a dry-pipe, pre-action system with high-temperature heads so that water enters the pipes only when the sprinkler heads open at higher temperatures than standard heads. This type of two stage dry-pipe system is currently installed in the Hydro Place data center. Two stage systems are recommended that trigger only when two zone sensors go off. Also, the pipes within the system should be welded together, not merely clamped, to prevent leaks and accidental flooding. Even with such a system, it is highly desirable to have a standby switch to abort firing of the system. A more desirable alternative to water-based fire suppression system is one based on the use of inert gases, such as an INERGEN gas system.

Currently the Hydro Place data center environment uses two air conditioning units on a manual control. While having two A/C units in the room is appropriate, automatically linking the systems through an electronic control mechanism is recommended so that mechanical failures can occur without an unacceptable rise in data center temperatures. Failure mode for HVAC should be open/full blast AC. Systems using chilled water often have separate external cooling or condenser systems, helping to ensure that there are at least two complete systems with no single point-of-failure.

From a capacity perspective the industry rule of thumb is to provide t=KW/20 of cooling capacity where t is the number of tons of cooling required. The KW usage will vary as the installed based of server and networking equipment in the data center changes. It is recommended that a review of HVAC capacity be conducted every twelve months to ensure adequate cooling capacity is available. No current capacity for the A/C units was provided by Hydro for the analysis.

Hydro currently has HVAC humidity monitors installed to avoid over cooling. Excessive cooling causes condensation on equipment, which is dangerous, while air that is too dry leads to excessive static. As well, separate venting for the Datacentre than for the broader building is preferred, as is currently provided in the Hydro Place location.

Another important issue to consider for HVAC systems is a load shedding protocol. This identifies when to turn off monitors and other heat and load generating equipment in the data center that is non-essential for continued operations.

8.5.1.4 Power Protection

It appears as if careful consideration is given to most core components to ensure they are at least connected to a surge protector. There should be more consideration to connecting UPS's to building UPS facilities or at least spreading the load across multiple outlets. Non-core infrastructure such as desktops, printers and laptops are often not protected at all and it appears Hydro has not given much consideration to protecting these components. For larger installations, such as Hydro Place and Churchill Falls, a single integrated UPS should be put in place to provide for three hours of operation instead of a three-minute graceful shutdown period in the event of a power outage.

8.5.1.5 Data Protection

The current technology being used for data protection is more than adequate for Hydro's current requirements. Although TSM is currently used throughout Hydro, there is a move away from this technology to a single backup solution. This consolidation should simplify support and administration of backups in the future. The selection of one vendor over another would be a function of an analysis of the file types, sizes and storage requirements for each type of data managed in the network. As such development of a Storage Strategy is recommended as a follow-up to this report, and would be included as part of the Storage Area Networks project.

Storage Area Networks

Storage Area Networks (SANs) are bringing a paradigm shift to how corporations look at their data and datacentres in general. For the last few decades corporations have prioritized and managed their data from the perspective of the server it was stored on, and viewed the power of their datacentres based solely on the CPUs and CPU cycles housed within. Through the centralization of management and storage of data, SANs are changing this mind set. With the addition of new SAN technologies such as storage virtualization, real-time data replication across large geographical areas, and true file sharing; servers are slowly being relegated into the realm of being a mere peripherals or interchangeable front end processors to the storage.

Storage virtualization allows corporations to span volumes across multiple storage enclosures regardless of the manufacturer or distance. For large enterprises this will allow for the dynamic allocation of storage across multiple datacentres.

Real time data replication brings a whole new dimension to data backups and disaster recovery. Data can be replicated in real time to another volume, storage enclosure, or geographical location, allowing backups to be done any time during the day, eliminating the need for down time or compressed backup windows. The ability to replicate the data across vast geographical areas means disaster recovery timetables can be measured in minutes rather than hours or days. In the time it takes to boot the servers at the backup site and get WAN circuits moved, a corporation can be back in business.

Clusters today consist of two or more servers being grouped together, with one server being designated as the primary and the other being designated as a standby fail over server. True file sharing refers to the ability to store one copy of a file or database and allow multiple servers (regardless of the OS) to simultaneously access that file. Clusters will be created in the SAN, not the server; servers will be grouped to present themselves as one true virtual entity. The performance of a specific application will be improved simply by dynamically allocating another slim line server into the applications cluster.

As technology continues to evolve, corporations are realizing that the “separate storage for each server” model that has dominated the history of computing, and the avalanche of new storage requirements will bury users in soaring management costs. In contrast, well-implemented SANs can create consolidated storage that results in a dramatic improvement in the efficiency of storage management. Ironically, this SAN-based level of efficiency is exactly what so many datacentre managers have been seeking for their server environments.

While the concept of fibre attached storage has been around for many years, it has been primarily used to offset the distance limitations of SCSI, and thus been primarily a hardware solution. Current implementations of SANs have gone through many evolutionary changes from those days. ***Gartner Group*** defines SANs as a two-layer technology. The first layer describes the hardware involved in implementing a SAN - the plumbing. The second layer describes the value added software involved in deploying, managing, and leveraging a SAN.

Currently connecting a tape library to a SAN has required some variation of a data router to do Fibre channel to SCSI conversion and to provide a point of presence for the library itself, while these devices are designed to perform at high speeds they still inject a bottle neck into the backup process. In the near future tape libraries (tape drives and tape robots) will be directly connected to the fibre fabric.

There is a lot of confusion in the industry with regards to SAN and NAS (network attached storage), quite often they are presented as competing technologies and architectures. NAS and SAN are complementary technologies and architectures both having a place within a enterprise computing environment. Where SANs are dedicated storage networks, NAS products are dedicated file-sharing appliances, or servers, not a network. Since the plumbing of SANs are block- or device-oriented a NAS appliance could attach to a SAN just as any other server would to access storage resources. Today most NAS products do not support the SAN management technologies that have been put out in the market, so NAS within a SAN remains a future direction. The following diagram illustrates generally where NAS and SAN would sit within an enterprise-computing infrastructure.

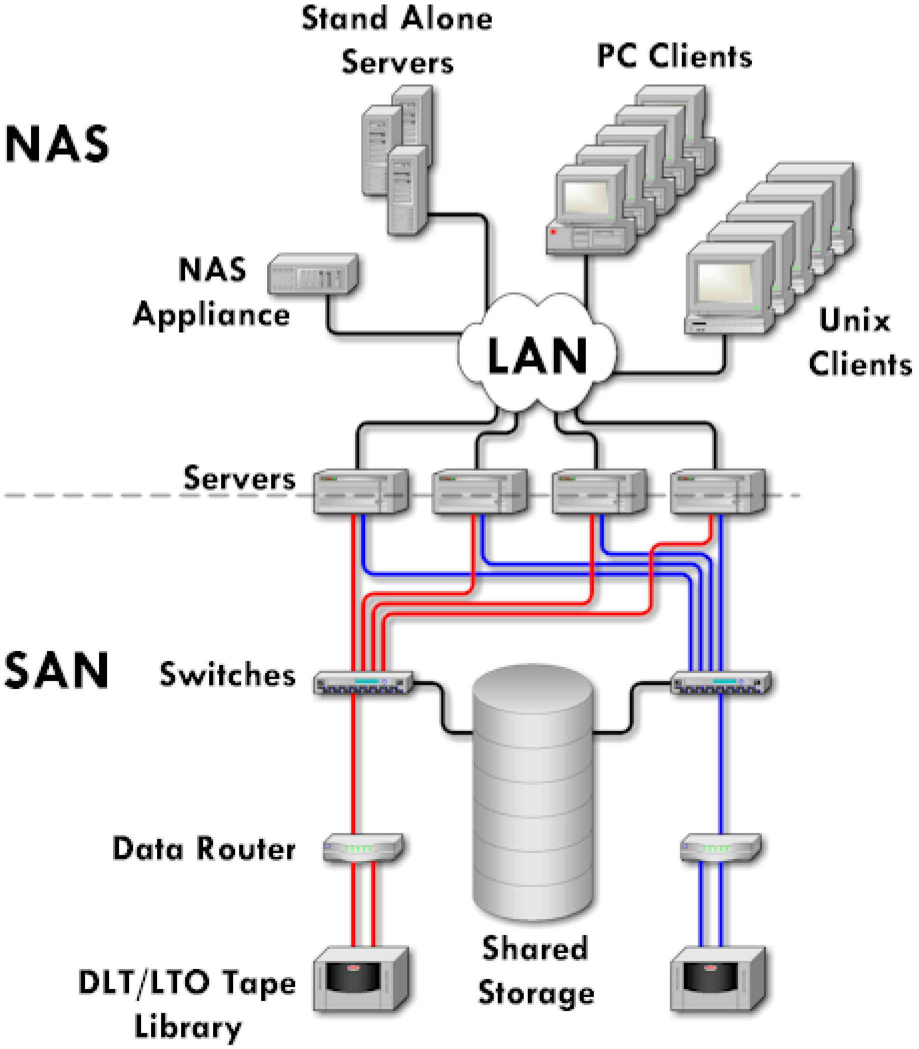


Figure 16 - Network Attached Storage and Storage Area Network

Given the importance a SAN would have within an enterprise, it must be constructed using a redundant fibre fabric having each server dual attached while tape backup libraries are single attached into the fibre fabric. The SAN management station is connected directly into the fabric to allow for inband management.

When deploying or migrating to a SAN it should be done on an application-by-application basis. Once the data is migrated into the SAN any new or replacement servers should be low profile rack mounted as the need for large storage capacity within a server enclosure has been eliminated by the SAN leaving only memory and CPU capacity to be accommodated. The SAN and SAN management environment must be housed within a controlled access environment as the uptime of the enterprise-computing environment is directly associated with the uptime of the SAN.

8.5.1.6 Operating System Software

As discussed in the LAN portion of the Short-Term Design, Windows NT Server as an Enterprise class operating system has gained a lot of ground in recent years. As Windows 2000 matures and is further enhanced it will provide the ideal foundation for Hydro’s migration from Windows NT. Hydro should follow the natural progression of the Windows NT Server OS to Windows 2000 and beyond.

8.5.1.7 End-User Infrastructure

As part of the long-term technical design there were two primary classes of users defined:

- Support Staff – Require some applications outside of standard office productivity, messaging and JDE. Support staff would be provisioned with laptops or desktops and utilize a thin client to access core network applications in addition to locally loaded software.
- Production Staff – Do not require applications outside of standard office productivity, messaging and JDE. Production staff would be provisioned with thin client appliances (WinTel) and utilize a thin client to access core network applications.

Due to this class of user definition there are two types of end-user infrastructure incorporated into the short-term technical design. The first of these is a thin-client based WinTel appliance. The thin-client appliance would be standardized across Hydro and would provide for standardized configuration, eliminate issues with alteration of end-user software image, and provide for ease of sparing, repair and troubleshooting in remote locations. In addition, a thin client appliance can easily be made accessible in a common area of Hydro workplaces to act as a kiosk for end-users who do not have a dedicated computing requirement for access to e-mail, Corporate Intranet, office productivity tools and other such services.

As part of the analysis of the short-term design recommendations, estimates were made of the mixture of support staff and production staff in each location. It was estimated that Support

Staff were located in Hydro Place and Bishops Falls, and that all other locations were primarily Production Staff. As such, this was used as the basis for developing the implementation plan for the end-user infrastructure. It is important to note, however, that the decision around the mixture of provisioning thin client appliances versus laptops or desktops does note materially impact on the overall design.

8.5.1.8 Printers

In some cases, the workgroup printers deployed are oversized for the number of people that use them. Hydro should focus efforts on appropriate location and sizing of printers to promote better usage of workgroup printers.

8.6 Security

8.6.1 Domain Access & Logon Security

Authentication is used to verify the identity of the user and to grant that user access to information. Once a users identity is confirmed in the computer system, access to all preauthorized resources (files, applications and printers for example) is granted. For Hydro this authentication is controlled primarily through the domain access and logon security. The first line of protection for the information residing on these computer systems is based in the strength or weakness of this process. Recommendations include:

- Password scheme that forces passwords to be at least semi-cryptic.
- Lock workstations with screen saver password when left unattended.
- Provide laptop users with lockdown mechanisms
- Both laptops and PDAs should be programmed with power-on passwords
- Use a two-factor password standard for access to the various computer applications.

8.6.2 Single Sign-On

Single sign on (SSO) is certainly the “Holy Grail” of information technology. Users know that they want SSO and what they expect SSO to provide. Single Sign-On is defined as having the following characteristics:

- Users gain access to the network, all systems, all applications and transactions through one authentication process.
- Electronic credentials are passed automatically between the various systems and applications, providing the necessary security access controls to corporate information.

wave recommends that Hydro establish a phased in approach to single sign on, based on the following approach:

- Establish a centralized password management system such as SecurID or PKI for a single sign on solution in the short term
- Establish a plan to minimize, within reason, the IT technologies used to provide future computer applications.
- Review developing SSO technologies to meet the needs and combination of technologies in place at Hydro.
- Implement a complete single sign on solution within 3-5 years.

8.6.3 Standard Workstation Operating System Images

The value of corporate information that now resides on workstations is increasing at an alarming rate. The inherent flexibility and functionality that makes a personal computer a valuable business tool also leaves this valuable information at risk. For these reasons generally accepted industry standards for security now include establishing a standard workstation configuration that is both secure and locked to ensure that users cannot make modifications.

One of the most important issues that **xwave** discovered during the technical review process is there is no mechanism in place to control the mutation of the standard image. Permissions must be set and controlled on the standard image such that users are not able to download and install unauthorized software. All requests for non-standard software should be made through the helpdesk and be reviewed on a case-by-case basis.

xwave recommends that Hydro modify the current standard images for workstations and laptops to address vulnerabilities and begin to deploy these new images during the ever-greening process. Since the ever-greening procedure is a long-term strategic process, if resources exist it may be prudent to develop an SMS package to address vulnerabilities and permissions in the immediate to short-term

It will be important to maintain this configuration and documentation as time goes on. Routine vulnerability assessments should be performed after additions to the current standard image. Routine assessments are discussed in a following section.

8.6.4 Standard Server Configurations

A base configuration is defined as being a minimal configuration with common applications installed. Common applications are applications that are installed on all servers regardless of the server's purpose. The development of the standard configuration should be performed in concert with a vulnerability assessment. As with workstations, it is important to develop specific installation guides and maintenance procedures (including change management procedures) for the base configuration.

Each unique server type will have it's own section in the Security Policy document with appropriate references to supporting documentation. In the case where a server only differs from the standard by a few non-standard applications, a subsection within the standard configuration policy will identify the specific server, identify the applications and provide a reference to a specific installation guide.

8.6.5 Internet Accessible Services

From a computer security perspective Internet access creates challenges to minimize the security risks to these Internet accessible servers while allowing the applications to securely function as planned. Typically, companies use a firewall as protection from the Internet. While this is certainly an effective and recommended tool, the effectiveness of a firewall is enhanced when it is part of an overall security design.

It is recommended that Hydro move the DNS/Web server to a DMZ off the Internet firewall as pictured in the figure below and centralize security rule set enforcement and logging at the firewall.

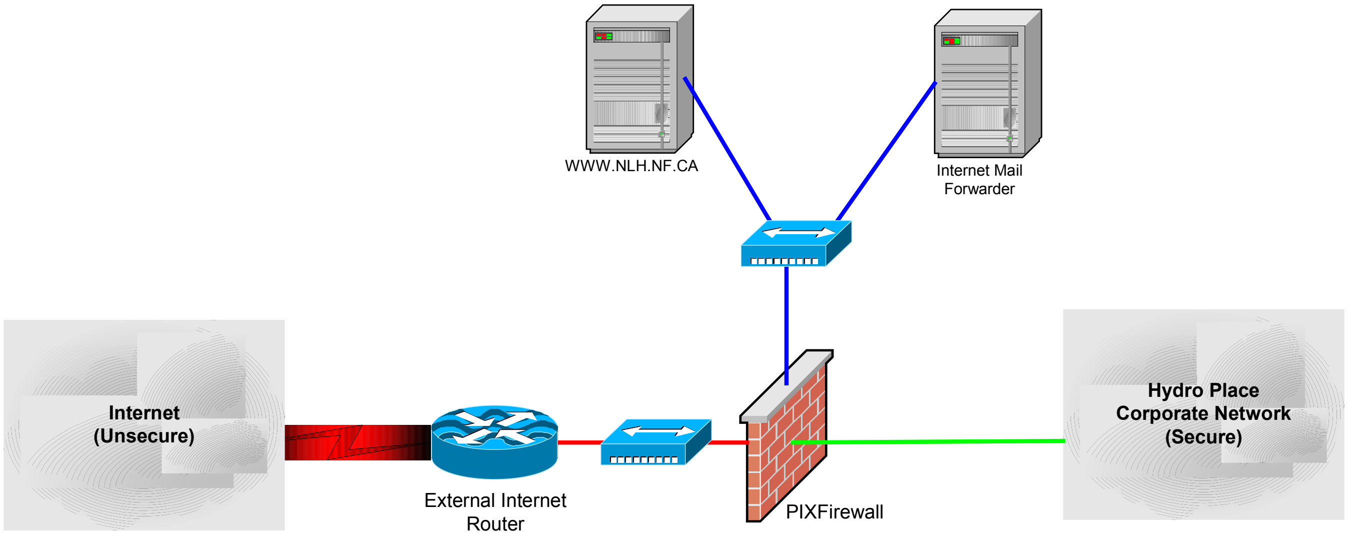


Figure 17 - Recommended Physical Connections for Internet Services Architecture

8.6.6 Internet Gateway

8.6.6.1 Firewall Type and OS Version

The current PIX Firewall is version 4.4(7), which is significantly out of date. It is understood by **xwave** that a hardware limitation is keeping the version from being upgraded immediately. It is strongly recommended that Hydro upgrade the PIX firewall software version to 6.0 when new hardware becomes available.

8.6.6.2 Firewall Security Policy

xwave has reviewed the firewall security policy configuration and has noted only three minor issues:

- No Port Address Translation (PAT) statement has been added to the PIX global configuration.
- The Internet mail receiving and forwarding service is located inside the Hydro network.
- ICMP is allowed to pass through the firewall from any source to any destination.

8.6.7 Internet Mail System

The role of electronic mail has grown in the past few years from a corporate luxury to an essential business tool. A critical part of this email infrastructure is the communications to Internet mail systems. Proper security controls on this mail service is a key portion of an effective security program.

From a security perspective the ideal design for a mail service includes two mail servers. One mail server would be located in a Demilitarized Zone (DMZ) to send and receive all email with the Internet. The second mail server would be within the internal private network and perform all inter office messages as well and send and receive all mail from outside the organization through the DMZ mail server.

It is recommended that Hydro move the external Internet SMTP forwarding services off the internal Lotus Domino SMTP Server and set up an Internet mail forwarding system in the DMZ to handle incoming and outgoing mail. SMTP anti-virus and content security software should also be installed on this server to scan both incoming and outgoing smtp connections for malicious or undesirable content.

8.6.8 Outbound Authentication and Logging of Internet Access

To minimize corporate liability and to ensure efficient use of the Internet is maintained, management controls are required. The generally accepted industry standard for employee Internet access includes an acceptable Internet use policy and monitoring Internet usage.

xwave recommends that in the immediate short-term, Hydro leverage the transparent authentication provided by Microsoft Proxy server to control and log outbound Internet access. Web caching will greatly improve the performance of Internet browsing as well as reduce WAN traffic to some extent.

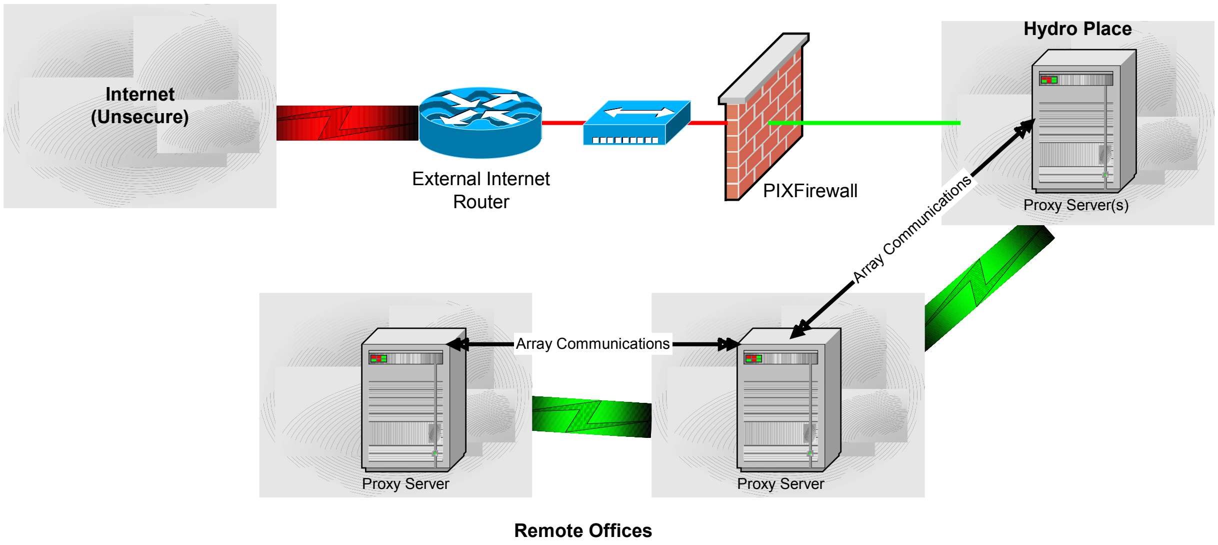


Figure 18 - Proxy Server Deployment

xwave recommends that Hydro configure at least three proxy servers (Churchill Falls, Bishop Falls or Port Saunders, and Hydro Place) in an array configuration to aid in the reduction of Internet traffic over the WAN. An array configuration also allows for redundancy in the configuration as the array can be given a single alias within DNS. The other alternative is to configure a proxy service at each site using the local file and print server and to have local users always access their own server.

The selection and design of methodologies should be examined further by Hydro before deciding on an appropriate solution. Due to the concentration of users within Hydro Place, it may be a good idea to configure at least two servers locally (referenced by a single DNS alias) to provide transparent redundancy for Hydro Place users.

Each of the Microsoft proxy servers has the capability to monitor and log all users access. **xwave** recommends that the log files from each proxy server be extracted in a flat file format to an SQL database for report generation. This consolidation of information will allow Hydro to create effective reports to analyze the organizations Internet usage and ensure that policy standards for appropriate use are adhered to.

8.6.9 Remote Access

8.6.9.1 Modems Attached to User Workstations

xwave noted many modems attached to user workstations during site visits and does not believe it is Hydro's intention to continue to allow the use of these devices. These modems should be retrieved from the field as soon as possible as they represent a significant security threat to Hydro.

8.6.9.2 Dedicated Dial Solution

xwave has examined Hydro's current remote access solution and in the immediate and short-term recommends a more secure solution based on SecurID tokens for positive authentication. Remote access at Churchill Falls should also be tied into SecurID by making the remote dial-up server there an Ace Client and by providing remote access users in that region with SecurID tokens.

8.6.9.3 Client-to-Site VPN Services

It is recommended that Hydro develop VPN services (leased or private) and provide employees who subscribe to high speed Internet services access to the corporate network via VPN. This will eliminate the potential for simultaneous connection to the Internet and corporate network, and the work from these home employees will see improved service levels.

A common authentication scheme for all remote access is desirable and therefore it is important when selecting or designing the VPN service to ensure that it supports the SecurID authentication mechanism currently in the design and development phase.

It is not recommended that VPN be deployed over dial Internet services without the use of terminal services, as encryption overhead will cause increased latency over an already slow dial connection. It is recommended that if Hydro proceeds with VPN deployment that a dedicated VPN tunnel server be provisioned when user subscription exceeds one hundred users. In this way, the processor and traffic overhead of VPN connections will not affect outbound Internet service performance.

8.6.10 Remote Vendor Support Services

Another element of the recommended short-term security technical design is to configure positive authentication for remote vendor support access wherever possible through assigning remote vendors unique system user IDs with appropriate permissions. Prevent remote vendors from changing modes to a generic user ID such as root is also recommended. As part of the ongoing Security Policy Hydro should perform accounting and auditing on the remote vendor's system access and make them aware that this accounting is taking place. An additional step would be to protect the log files associated with this accounting from erasure and modification by anyone except Hydro administrators. Review log files should be conducted regularly to ensure that only authorized systems and files are being accessed.

8.6.11 Anti-Virus Configuration

Due to the prevalence of malicious computer viruses and their potentially detrimental impact in the computing environment, a means of virus management and risk reduction is essential in today's workplace.

It is important that any organization attempting to employ an effective virus solution have the following:

- A virus policy
- An escalation procedure
- Adequately trained people to manage the solution

In the event that a virus incident occurs, it is imperative that all personnel are completely aware of their roles and responsibilities during the entire process. An escalation procedure will clarify both the responsibilities as well as the actions to be taken given depending upon the severity of the situation. A clearly defined process will greatly reduce any possible damage as well as avert a corporate embarrassment.

Hydro's current investment in Norton Anti-Virus CE 7.5 makes the migration to an alternate solution prohibitive for the duration of the current licensing agreement. Also the Symantec product offering is very robust and flexible such that there is only limited advantage to changing vendors.

8.6.12 Routine Vulnerability Assessments

xwave strongly recommends that vulnerability assessment tools be run against at least critical devices on a periodic basis of not longer than a few months. Internet connected edge devices and publicly accessible servers should be scanned even more frequently than internal network devices.

A penetration analysis (test) should be conducted periodically at least twice yearly and whenever major changes are placed into production. The IT Security Policy should address the frequency and scope of penetration analysis testing. Testing methodologies and tools as well as results and recommendations should be well documented by any outsourced third-party who performs the testing.

8.6.13 Logging and Log Data Presentation

xwave believes in the philosophy "log everything within reason". This means that security systems should:

- Log at both the network and application layers at edge devices.
- Log all authentication requests.
- Audit operating systems for significant events such as administrator access, system file deletion or modification, etc.
- Log system application debugging and error messages.

As well, OS logs, network device syslogs, application logs, and change management logs can be useful for:

- Usage trend analysis
- Identifying user training requirements
- Aiding in prosecution of malicious attackers
- Reverting to a previous working state in case of problems

Maintaining the integrity and accuracy of system logs by limiting access to this information through the use of properly configured file system permissions is also very important.

Although **xwave** recommends that Hydro centralize and automate logging as much as possible it is not possible given the wide variety of applications and technologies in use to completely centralize logging facilities. Distributed logging mechanisms to gather data are often quite practical while distributed reporting and presentation systems are usually not. **xwave** recommends that Hydro centralize reporting and presentation of log data gathered from distributed operating systems, firewalls, routers, and IDS agents as much as possible. This design will be developed with long-term strategy in mind and will be modular to allow for ease of additions in functionality. Since no one product currently exists on the market that addresses reporting for the complete suite of Hydro hardware and software, it will be necessary to develop a custom front-end HTML reporting server and SQL server that will query the distributed log databases for presentation information. The desired system is comprised of components as follows:

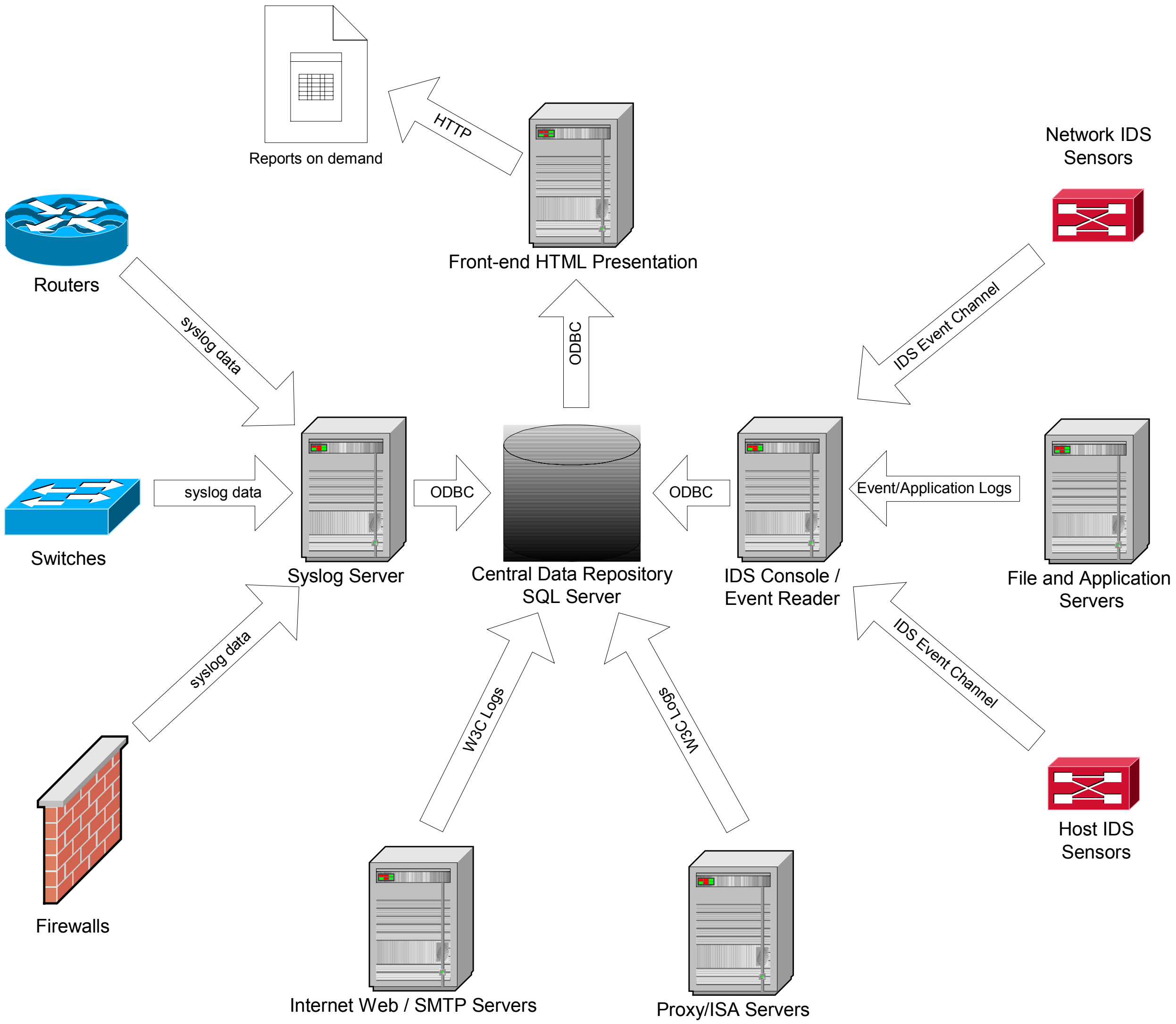


Figure 19 - Logging System Architecture

8.6.14 Active Intrusion Detection

Real time intrusion detection provides a means to react to situations when the internal network's security is under attack or has been breached. Secure networks need an application that is highly customizable to allow an administrator to adapt predefined attack patterns to new variations. Active intrusion detection systems have become accepted as industry standard, logical complements to firewalls.

IDS systems allow administrators to monitor, recognize attack patterns (signatures) and automate responses to these events. When weighed against the cost of Internet or internal system extended down time and lost or destroyed corporate data, the investment required for a real-time intrusion detection system is justified.

xwave recommends that in the long term, Hydro employ numerous network, host, and hybrid Intrusion Detection Systems (IDS) to detect and respond to suspicious activity. This IDS system should be strategically located with the internal network, on the DMZ and integrated with key servers. Attached is a diagram displaying key locations for IDS sensors.

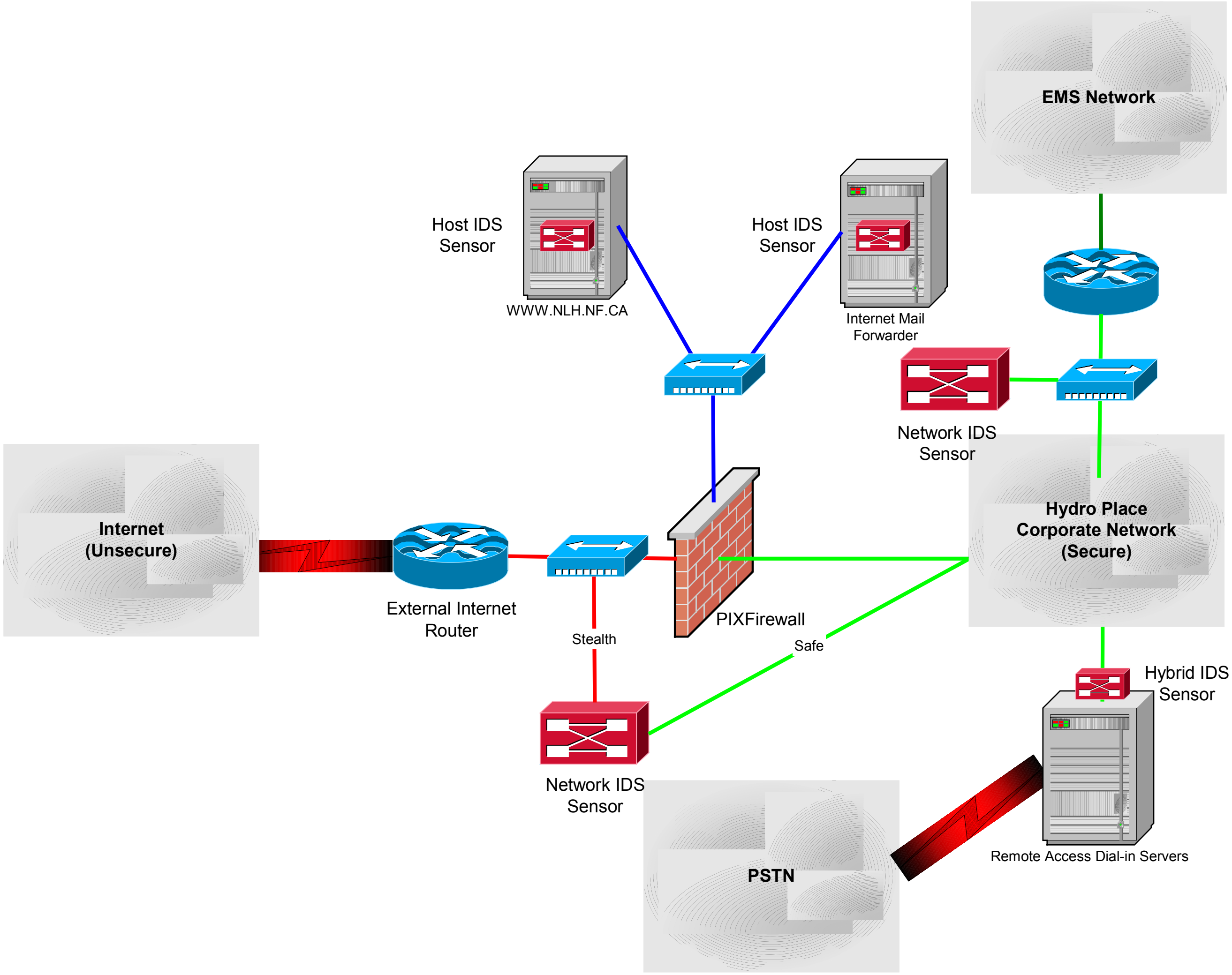


Figure 20 - Potential Deployment of IDS Sensors

8.6.15 The Corporate IT Security Policy

A security policy is the key foundation to a comprehensive security program. The security policy should address; management ownership, a risk management review process, process to approve exceptions to the policy, technical standards for all technologies and a process to update the policy as technology and business environments change.

8.6.16 Configuration and Change Management

xwave recommends that Hydro develop and maintain a dedicated online data repository for all configuration and security related information pertaining to Hydro IT assets. There is potential to develop this system on the same hardware as the logging database and front-end server.

Considering the size of Hydro's network as well as the scope of work that change/configuration management envelops, at least one dedicated Change Management Coordinator and Custodian will be required to organize data, update forms and approval routing procedures, and enforce change management procedures. In other words a keeper of the system is required and recommended.

To support Hydro initiatives such as ever-greening and to maintain Hydro at the optimum configuration for each device, it is important to maintain sufficient test lab equipment representative of Hydro's computing environment.

Hydro will need to develop a change management procedure with appropriate approval routing for each subsystem of the IT infrastructure. Final change authorization is held by the Change Management Coordinator who will grant approval only when all supporting documentation has been submitted (test results, updated end-user documentation, prior approvals, etc).

8.6.17 Disaster Recovery and Business Continuity

It is **xwave**'s understanding that Hydro is currently involved in drafting a high-level Disaster Recovery and Business Resumption Plan. This is an important first step and serves as an indication that Hydro senior management recognizes the importance of business continuity in the event of a disaster affecting Hydro Place. In order to fully appreciate the risk involved in maintaining a computing system without appropriate consideration for disaster recovery, a full risk analysis that specifically addresses the impact of a disaster scenario is required. **xwave** recommends that a detailed Business Impact Analysis be commissioned by Hydro to help senior management and individual business units to better understand the overall impacts and probable risks that could have the greatest impact on the company's business operations should a disaster occur. The results of a Business Impact Analysis allows for well-informed management decisions. Once the Business Impact Analysis has been completed, a Disaster Recovery plan can be developed

8.6.18 Bill C-6 Compliance

As part of the security review **xwave** was asked to make recommendations to allow Hydro to become compliant with the Federal Government Policy, Bill C-6. In making these recommendations, however, it is important that Hydro perform its own legal review of requirements of Bill C-6 to ensure compliance. That is, **xwave's** recommendations are of a technical nature, and are not meant to imply a legal opinion on compliance.

At the heart of the Federal Government legislation is premise that information collected by a corporation from its various stakeholders (employees, customers, partners, suppliers, etc.) must be collected, stored and used only for the purpose identified, and only with the consent of the stakeholders. With this in mind it is important to conduct an audit of personal information collected by the company, including points of origin, storage and security measures, and consent. **xwave's** review of current practices showed that there has been some work performed within Hydro from an employee perspective, with a specific view to new hires, but that customer and long-term employee information has not received sufficient attention to comply with Bill C-6. With this in mind Hydro's legal department should undertake a review of personal information that can and/or cannot be collected and stored in electronic format, and provide guidelines around protection measures that must be put in place to safeguard this information. It is anticipated that such a review will result in numerous changes to Hydro business processes in dealing with its stakeholders.

8.7 Network Management

As IT infrastructure continues to be integrated further into the mission-critical operation of a business, there is an increasing requirement to proactively monitor and manage all of the elements of the infrastructure from a service management perspective. Service Management is the management of IT services and the business processes that are dependent on these services.

Though frequent or lengthy IT service outages are not currently a problem for Hydro, the potential exists for significant outages in the future since, as defined in the Vision, Hydro's IT infrastructure will play an integral role in supporting a unified network for both the production and support functions. As a result Hydro will face new challenges in ensuring the integrity, availability and performance of all IT services.

Currently, there is very little in the way of "formal" Network Management at Hydro. This must be contrasted with the network management rigor and processes defined for its Energy Management System (EMS), where all aspects of remote monitoring and control of the power system are well planned, documented and operated on a 7/24 basis. In essence, Hydro has built in its prototype Network Management System through its EMS. Hydro must move to implement this same level of information gathering, proactive maintenance and control in its IT infrastructure.

Given the fact that no "formal" Network Management solution currently exists within Hydro, there is a great opportunity to develop a solution "from the ground up" using the information and requirements that were uncovered through this assessment of Hydro's IT environment.

8.7.1 Developing Availability and Performance Management Policies

Most of the recommendations for effectively managing the components comprising the Hydro IT environment revolve around the development of policies and processes that dictate how availability and performance management will be delivered. This can take the form of a global IT management policy for which there is a section dedicated to each component or it can take the form of a separate policy for each. Regardless of the approach taken, the specific means for providing availability and performance management for the various components of the IT environment should be documented (e.g. as Service Level Agreements) and reported against on a regular basis.

An availability and performance management policy should include the required service level objectives that the IT infrastructure must meet and will serve as a blueprint for how the network infrastructure components will be managed. Standard items that should be included in the development of such a policy are:

- Establish availability objectives
- Establish performance objectives
- Establish incident management workflow processes

- Define how often availability reports will be produced and who should have access to these reports.
- Define how often performance data will be analyzed for trends and reports produced and who should have access to these reports.

8.7.2 Network Elements

8.7.2.1 Switches, Routers and Hubs

Along with the physical cable plant, the hubs, switches and routers provide the network backbone upon which all other IT systems and services are built. Since all IT services share the same network, it must be built and managed such that it provides "bullet-proof" reliability. Any incidents occurring within the network must be rapidly identified in terms of what services are affected, and corrective actions prioritized accordingly.

The recommended technical solution that will provide these features for the Cisco switches, routers, and hubs is known as SmartWay 2001. SmartWay 2001 is a solution set that includes several products which are tightly integrated with one another to provide a true end-to-end service management view of the network. The core components of SmartWay 2001 are Cisco's CiscoWorks 2000, HP OpenView Network Node Manager (NNM), and HP OpenView Operations (OVO).

8.7.2.2 Circuits

The circuits linking the various Hydro sites are essential components for the monitoring and management of the IT infrastructure. As such, it is recommended that all circuits be monitored using the same Enterprise Management server used to monitor the network elements.

While it is usually not possible to monitor telecommunication service provider owned devices within leased line circuits, the end-to-end availability and performance of these circuits can be monitored using the end-point devices owned by Hydro.

8.7.2.3 Internet

As the Internet will play a larger role going forward with the adoption of VPN services, Hydro requires information on a regular basis to validate the performance of this component of its network.

It is recommended that Hydro pursue the possibility of establishing a Service Level Agreement and obtaining reports on the performance and availability of its Internet Service Connection provided by Rogers Cable.

At the same time, however, basic performance information can be gleaned from the PIX firewall itself. This approach allows Hydro to collect data from its own equipment and produce its own reports on the availability and performance of the Internet link.

HP OpenView NNM can monitor the PIX firewall for availability of both the device itself as well as the status of each interface on the PIX, including the Internet interface. If the Internet link were to go down, HP OpenView NNM would detect that the Internet interface on the PIX has gone down. It is important to note that this level of monitoring will only inform Hydro of problems with the physical connectivity on PIX's Internet interface; it cannot detect problems on the provider's side of the link.

In terms of performance, HP OpenView NNM can collect information relating to bandwidth, packet loss, and PIX memory utilization from the PIX itself via SNMP. This information can be monitored for certain thresholds in real-time or stored for historical analysis and regular reporting. If this is desired, the appropriate security measures should be enacted on the PIX to ensure that only the Enterprise Management server can access information on the PIX via SNMP.

8.7.3 Infrastructure

8.7.3.1 Windows NT/2000 Servers

Defining a management policy for servers is more complex than that undertaken for the network infrastructure elements. This is due, primarily, to the wide range of services provided by a typical server. There are various layers to which management could be extended such as:

- Simple network availability (or up/down monitoring)
- Hardware health (failed hard drives, overheated CPU, etc.)
- OS health and performance (disk drive space free, paging rates, CPU utilization)
- Application health and performance (# active sessions, response time, etc.)

At a bare minimum, the availability and performance management policy should cover simple network availability and hardware health. To facilitate this approach, the servers should be SNMP enabled and added to the HP OpenView console. This would alleviate the need for the "Server Alive" program, while at the same time, ensuring that the servers are monitored for availability on a 7x24hr basis. Enabling SNMP on each server and installing vendor-provided agents (e.g. HP NetServer Agents) would allow hardware-specific alarms to be incorporated into the 7x24hr-monitoring regime.

In order to monitor, manage and report true service levels, however, all of the above layers must be addressed. One product included in the recommended SmartWay 2001 solution for management of the network elements, HP OpenView Operations, provides the capability to monitor all layers of infrastructure on servers through the use of an Operations Agent distributed from the management station to each (client) server. These agents communicate via secure, reliable communication mechanisms with the management station. In addition, they can function independently from the management server, performing advanced local event filtering and corrective actions to predefined incidents.

To provide the data required for performance monitoring, trend analysis and capacity planning, a complimentary Performance Agent should be distributed to the (client) servers. These agents collect baseline and historical performance data for future analysis, but can also proactively monitor performance thresholds, alarm to the management station and/or perform corrective actions locally.

For specific applications and services, there are a number of “SMART Plug-Ins” available that work in concert with the Operations and Performance Agents to provide in depth remote monitoring and management.

Databases and e-mail/groupware services are not the only applications that can be effectively monitored. Internet sites are becoming more and more "mission critical" because of the boom in e-commerce. Businesses are finding it imperative to minimize downtime to maximize customer purchases. Application management can provide preemptive warnings of impending problems, reducing down time and increasing business success.

Another product included in the recommended “SmartWay 2001” solution is HP OpenView Internet Services. This product enables staff to efficiently predict, isolate, diagnose and troubleshoot problem occurrences, anticipate capacity shortfalls, and manage and report on SLA’s for servers providing Internet services such as DNS and HTTP.

8.7.3.2 AS400

The assessment exercise uncovered the fact that there is currently a good level of performance data collection occurring on the AS400 system. It was apparent, however, that the information provided/reported on the daily paper report through this collection was not well understood. By developing an availability and performance management policy for the AS400, more meaningful information can be produced. All data collection and reporting requirements, including the purpose and audience for the reporting deliverables, are defined in advance of implementation.

In developing an availability and performance management policy for the AS400, a similar strategy to that recommended for the Windows NT/2000 servers can be pursued. That is, the management scope can be limited to simple network availability or full management capabilities can be implemented.

In the first approach, the AS400 can be monitored from the Enterprise Management server using HP OpenView NNM for availability status on a 7x24hr basis. To complement this availability monitoring, the current performance data collection and reporting strategy can be reviewed to ensure that the metrics being reported on are understood and that the report allows system administrators/business managers to ensure that the AS400 is meeting its service level objectives. To pursue full management capabilities, it is recommended that the AS400 be included in the Enterprise Management strategy.

8.7.4 Desktop Infrastructure

In similar fashion to the Network Management System infrastructure on the server side, the use of Network Management tools on the desktop infrastructure is in its infancy, but moving in the right direction. Currently Hydro is using Microsoft SMS as a tool for managing licensing on desktop infrastructure and selected use by the helpdesk to take control of end-user PC's for troubleshooting. As well, SMS is being tested for use in pushing system and configuration updates to the desktop.

Overall Hydro should continue to pursue implementation of SMS as its primary method of controlling the installed base of end-user systems. To maximize the benefits of using SMS and achieve the greatest ROI, the inventory and change control aspects of SMS should be analyzed and implemented in conjunction with an integrated Service Desk product such as HP OpenView Service Desk.

Hydro helpdesk support technicians use HP Desktop Tools to aid in trouble shooting hardware components at the desktop level. Although a good first approach to diagnose problems it sometimes has problems detecting intermittent problems on all hardware components. The implementation of HP OpenView Service Desk will greatly enhance the capabilities of the support technicians in responding to incidents due to its high level of integration with other HP OpenView products, HP TopTools, and SMS; as well as its integrated trouble ticket, inventory, change control, work assignment and problem history repository features.

8.7.5 Applications

Although a review of application performance was outside the scope of this study, there is significant need to incorporate applications management into the proposed Enterprise Management solution. Applications are a critical component of IT services and cannot be ignored if a true Service Management model is adopted by Hydro.

Applications typically have one or more server components, as well as a client component. There are several add-on modules to HP OpenView Operations and Performance for monitoring the availability and performance of the server components of the applications in use at Hydro. In addition, complementary products will allow the monitoring and management of the JD Edwards application residing on the AS/400 server.

Should the full end-to-end response time for any applications in use at Hydro be desired, there are two products which will assist in the monitoring and collection of performance related information for the desktop portion of application transactions. One involves modifications to the source code of the application in order to instrument it for response time measurements based upon the Application Response Measurement (ARM) API standard. The developer's toolkit (which includes run-time subroutines and code snippets) are free from HP. The second method to instrument applications for response time measurement is a product which allows encapsulation of existing applications in order to measure response time without modifying application code. This product is the HP ResponseTime Workbench.

8.7.6 Environmental Monitoring

Currently there is limited environmental monitoring and no remote management for elements of the Network and Server infrastructure. That is, there is no automated alarming or control for heating and cooling, access control, etc. to allow remote administrators to see the health of the environment.

Hydro should establish an environmental management policy that identifies which devices have embedded environmental monitoring capabilities, and where (if anywhere) environmental systems should be implemented to monitor the physical locations where mission-critical IT infrastructure is housed. Hydro should then enable embedded environmental monitoring capabilities on each applicable device. If physical environmental monitoring systems are to be implemented, ensure that they are manageable via SNMP or have a dedicated management strategy that can be integrated into the Enterprise Management solution in the 7x24hr operations monitoring facility.

8.7.7 Overall Solution Description and "Best Practices" Recommendations

8.7.7.1 Overall Solution Description

In terms of the proposed technical solutions for managing Newfoundland Hydro's IT environment, the key concepts are:

- Adopt a Service Management model for IT infrastructure to enable monitoring and reporting of IT services from a business perspective.

- Establish a 7x24hr operations are where alarms from the network devices, servers, applications, etc. are received and acted upon according to pre-defined availability and performance management policies and processes.

- Establish an Enterprise Console for centralized management of all elements of the IT infrastructure (i.e. single-pane-of-glass view).

- Enable devices to be managed through configuration of embedded management capabilities (e.g. SNMP) or through the installation/configuration of specialized management agents (e.g. HP OpenView Operations Agent, HP OpenView Performance Agent, SMART Plug-Ins).

- Implement an integrated Service Desk product (e.g. HP OpenView Service Desk) to enable configuration, change, incident and problem management functions to be performed in concert with the availability and performance management functions.

- Implement a Web-based Service Information Portal with automated report generation to provide appropriate information to IT and business stakeholders.

The following diagram illustrates the proposed technical solution at a high level:

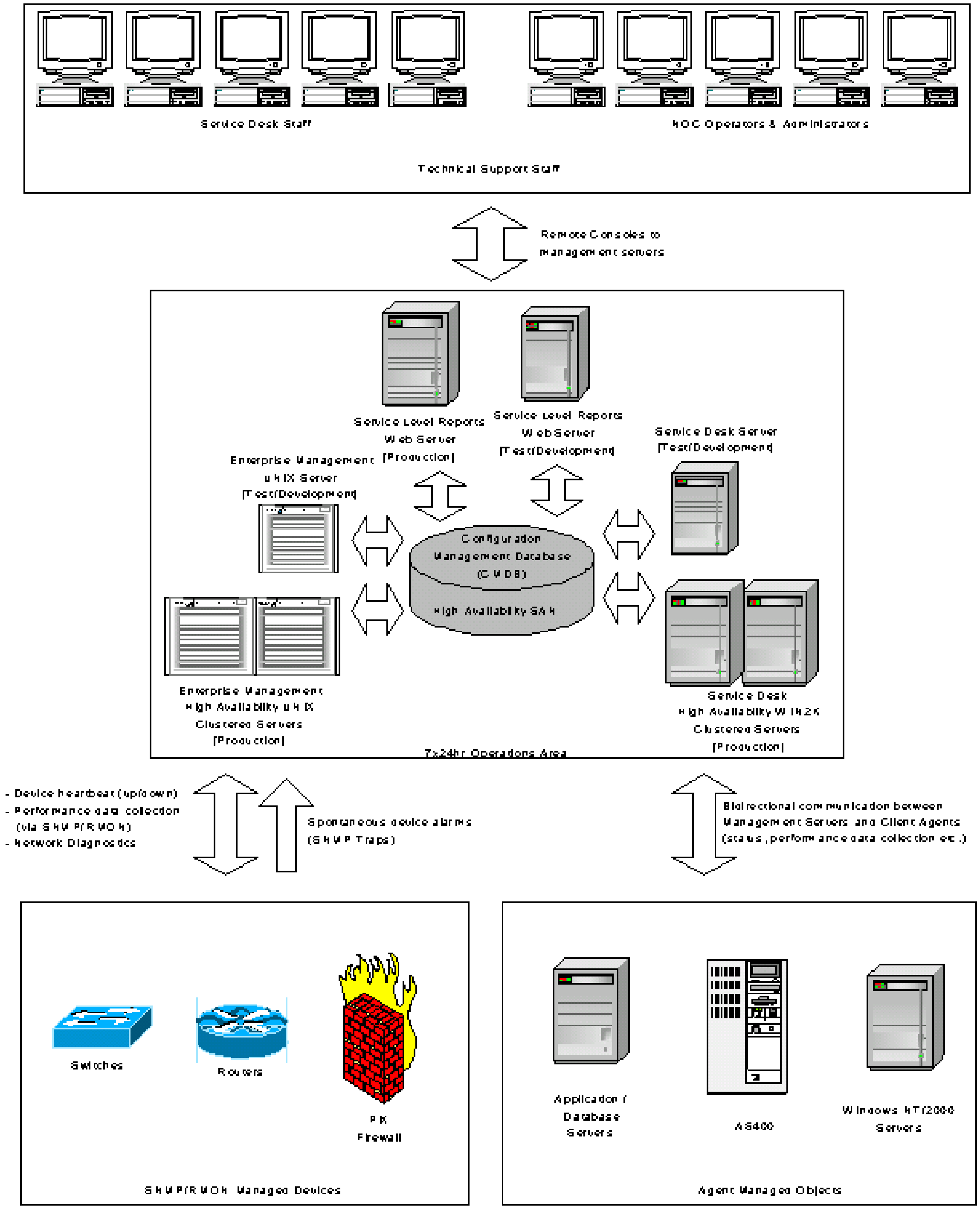


Figure 21 - Proposed Network Management Architecture

Two items shown in the above diagram that are not specifically addressed in the previous sections are the reporting server(s) and central data repository (configuration management database). As stated in the guidelines for developing availability and performance management policies, the key deliverables are the reports that reflect to IT and business managers how well the IT infrastructure is meeting the business needs. In order to fulfill the reporting requirement, the proposed network management solution must provide a mechanism for manipulating the raw data (whether availability or performance) into the appropriate end-user reports.

In the short term, the various report deliverables could be delivered through any tool that has the ability to obtain and manipulate data through ODBC (e.g. Microsoft Excel). It is recommended, however, that HP OpenView Reporter be used to produce the various reports and that these be delivered using the HP OpenView Service Information Portal.

8.7.7.2 “Best Practices” Recommendations

Prior to the acquisition and implementation of technology occurring, a formal requirements analysis, with adequate emphasis on people and process issues needs to be undertaken to increase the level of success.

The adoption of a Service Management model for IT should be based upon best practices such as those documented in the IT Infrastructure Library (ITIL) standard. The development of processes for Newfoundland Hydro based upon this standard will help ensure that the technology solution implemented meets the process requirements of the business, and not the other way around.

Once policies have been developed for each infrastructure component to be managed, the process of matching the needs of these policies against the capabilities of the proposed network management solution can begin. The specific network management solutions recommended in this document are considered best of breed in their specific area of expertise and should be more than capable of supporting the policies developed.

Another area of focus should be on prioritizing which IT infrastructure components need to be managed. The development of availability and performance management policies should begin with those components having the greatest priority.

One final “best practice” recommendation that should be considered for the proposed network management solution is to provide access to the solution for system administrators. In describing aspects of the proposed network management solution in the previous sections, the only “users” of the solution implied where those watching the Enterprise Consoles in the 7x24hr operations area. To expand upon the value that this solution can provide, remote access into the various consoles must be provided to system administrators.

8.8 Benchmarking and Performance Metrics

One of the key deliverables in the report was the creation of benchmark performance metrics and bandwidth utilization information. CPU and memory utilization peaks are not available from the current Network Management System. It is recommended that these factors be included in a network health trending process, and that the information be reviewed on a quarterly basis once the Network Management System is constructed.

8.8.1 Router sizing

The data shows peak busy hr traffic of 700M bytes during the busy hour of the busy day, which translates to approximately 700 packets/second. The specifications on the installed 7206 router indicate it can support the WAN without problems at a 1 Gbps backplane. Notwithstanding, depending on the amount of LAN traffic routed with Hydro Place itself there may be a sizing issue with the router. At Hydro Place the migration to a layer 3 switch and the elimination of the token rings will significantly reduce the demands on the 7206. It is expected that 7206 will support the traffic demands of future applications for quite some time.

Other routers will be run through a similar analysis once future applications possibilities are forecasted. Consideration of QoS support and survivability will be a key parameter in router model selection.

8.8.2 Bandwidth Consumption

As part of the bandwidth consumption measurement packet sniffers were placed on Hydro's network inside both the LAN and WAN environment to measure specific activities associated with application activity.

In order to find the mean traffic user by JDE per user filtering techniques were applied to capture traffic while sessions were in progress. Overall very low traffic was noticed, the utilization was 1.38% of the available 115.2 kbits/s of bandwidth =1.6 kbits/s per user on JDE. This correlates to some degree with the number provide by IBM (1.2kbits/s) in their 1997 report.

Mail

Two mail files were transferred during the study: one 601k file and a second 4021k file. As would be expected the traffic is quite directional and both files consumed the similar amount of bandwidth during their transfer. Data was filtered during the center of the 4021k file transfer to determine a mean steady state bandwidth utilization. The bandwidth consumed to St. John's during the file transfer was 88.48% of the 115.2k circuit and remained at this peak during the entire file transfer. Not surprisingly this type of traffic has the potential to fill pipes and congest the network.

One observation is that this type of traffic needs either traffic shaping or prioritization to ensure that other traffic remains unaffected by this size of mail transfers. Although large size files may be infrequently transferred over the network, the impacts could be significant if they were to take place during interactive busy hour. On a go-forward basis with a potential for a VoIP call on the WAN the impacts could be quite serious.

File transfers

The next test saw the same 4021k file transferred across the WAN. The traffic is quite directional and the file consumed 96.25% of the bandwidth toward St. John's while only 1.87% toward Whitbourne.

As was seen previously, this is a similar to the amount of bandwidth consumed during mail transfers. Again this would cause congestion if it were to take place during interactive sessions.

Http

The volume of web traffic consumed by a person accessing the Internet differs based on the complexity of the sited visited. Measurements were made on several typical sites and bandwidth calculations are as follows:

Five sites were visited and the returning traffic to the querying terminal was measured at 466131 bytes, or an average of 93k bytes per page for both transmit and receive. Based on this calculation a 256k pipe would provide 3 second response time to the average user, assuming no congestion through the network. If one assumes that it takes approximately 30sec to view the information on an average page the average surfer would consume an average 25k during constant high bandwidth surfing.

8.8.3 Wide Area Network Bandwidth Determination

In order to design a long term WAN for Hydro, one must establish the projected bandwidth requirement between sites. This will the drive the circuit sizing and type, router model and the software needs to handle the bandwidth demands. This bandwidth calculation begins with the evaluation of both current and future applications that are expected to traverse the WAN.

A list of both existing and future applications was compiled. These were then categorized into type, priority & whether or not they traversed the WAN. These were then classified into the following areas:

- High Priority,
- Interactive,
- Low Priority,
- Overhead and
- Non-applicable.

They were also separated into traffic types that traverse the WAN and LAN or those that traverse the LAN only. The data used to determine the bandwidth of the existing WAN and the potential future bandwidth demands came from two sources, measurements and consultation with application vendors.

In order to benchmark the existing applications data was collected on two cross sections of Hydro's private network. Typical applications were run and data was collected. This data was later analyzed to provide typical per user application bandwidths of the existing core applications seen on Hydro's WAN.

Vendors with expertise in the video streaming, JDE One World, security cameras, video conferencing, and SCADA type traffic were consulted to assist in establishing WAN bandwidth requirements for each specific application above.

The calculation of average bandwidth consumption per user was completed using information provide from the user survey. The per app/user bandwidth measured was weighted with the percent daily usage per application derived from the survey. It was determined that the total mean traffic demand per user is **2kbps** for the core interactive applications.

This, however, cannot be used as the basis for WAN bandwidth sizing in the long term. The bandwidth projections for the future must be based on daily worst case and projected future application demands. It is predicted that in the long term Hydro's interactive traffic type will be predominantly IP and consist mostly of http and thin client queries from an interactive perspective.

The calculation of future bandwidth consumption per user was estimated as follows:

- In the worst case scenario all users could be using http and if we assume 100k bytes per html page and one assume that the it takes approximately 30sec to digest the information on an average page the average surfer would consume an average 25kbps during constant surfing. This peak figure will be used for the long-term user requirements for interactive WAN applications. The other dominant traffic consumer would be the JDE One World, which consumes 12k-15k bits per second in a thin client environment.

Summing the average bandwidth per user and other multimedia or special apps give potential peak traffic during the day.

As bandwidth is purchased in specific increments there will generally be more bandwidth available than required for the interactive & high priority applications. This surplus bandwidth will be utilized by the low priority traffic (mail & file transfers). This assumes of course that the QoS will be implemented on the WAN. Based on the above assumptions, the long term bandwidth forecast was developed for sizing routers, circuit costing and confirmation of router hardware requirements.

The table below reflects the information gathered to support the estimates:

Location	LT bw/site
Stoney Brook	354.000
Springdale	434.875
Deer Lake	458.3125
Wabush	504.0313
L'Anse Au Loup	515.75
Stephenville	539.1875
Port Saunders	882.625
Whitbourne	586.0625
St. Anthony	586.0625
Happy Valley	1068.969
Bay D'Espoir	1302.188
Bishop Falls	1746.344
Holyrood	1629.156
CFLCo.	1979.563
St. John's	2988.000

9.0 Integrated IT Management Plan

This IT Technical Architecture Strategy Report presents the recommendations required to achieve a reliable, secure and cost effective networking and processing architecture that provides adequate performance to meet Hydro's needs. However, a critical determinant of a successful infrastructure program is an ongoing IT Management Plan. The two key elements of this management plan are:

- Management Processes
- Evaluation and Refresh Cycle

Management Processes

The first element of the IT Management Plan involves the implementation of appropriate processes to facilitate the ongoing operation and coordination of the IT function at Hydro. The IT Infrastructure Library (ITIL) methodology for IT management plays a significant role in this regard, as it outlines the primary Operational and Tactical Management processes required by an IT organization to effectively manage their IT infrastructure. To this end, the ITIL framework applies directly to the processes Hydro requires to manage the ongoing operation of its IT infrastructure.

Operational Management

Based on the ITIL framework there are five Operational Management components that must be considered:

- Change Management
- Release Management
- Configuration Management
- Incident Management
- Problem Management

From Hydro's perspective, there are established activities to address certain elements of Problem Management, Configuration Management and Release Management through the provision of helpdesk services, standard images, etc. As well, there are isolated efforts around Change Management. These activities are noted in the relevant sections of the Information Technology Technical Architecture Strategy Report.

The major shortcoming of the current approach is the lack of centralized coordination and standardization of these operational management efforts. Hydro's investigation of an ITIL-based IT management system to coordinate the various silos currently involved in these operational processes will begin to address this shortcoming.

Tactical Management

Again, using ITIL as a framework, there are five Tactical Management components that must be considered:

- Service Level Management
- Availability Management
- Capacity Management
- IT Service Continuity Management
- Financial Management for IT Services

It is recognized that the effective implementation of these Tactical Management aspects is predicated on the successful implementation of the Operational components to act as a data gathering and storage repository for management information. As with the Operational Management components, there are currently activities underway within Hydro that address portions of these requirements, but there must be a formalized, centrally managed process to ensure proper accountability and interoperability. Again, ITIL provides one potential framework for implementing this process.

Evaluation and Refresh Cycle

The second element of the IT Management plan is an Evaluation and Refresh Cycle. This cycle is intended to support the ongoing planning and development of the IT infrastructure to ensure that the strategy outlined is this report is a “living plan”.

The evaluation and refresh cycle should balance the opposing drivers of minimizing cost / effort and maintaining currency of the plan. Smaller “course corrections” made at more frequent intervals tend to be easier to implement that large changes in direction made infrequently. Opposed to this, however, is the cost and effort associated with reviewing the plan when there has not been sufficient time elapsed to provide for material changes in the key technology and business drivers.

In addition to this consideration, there are varying levels of evaluation and review that can be undertaken. They can be generally classified into the following types:

- **Directional Review:** A directional review is the smallest type of a review that can be undertaken. Under a directional review the major recommendations of the plan and the associated implementation plans are reviewed by the senior and functional managers to identify any areas where there have been material changes in the key technology or business drivers that gave rise to the recommendation. This can usually be accomplished in a one to two-day review session and can be coordinated by the document owner.

- **Sectional Review:** A sectional review involves a more detailed investigation of each of the research areas, such as Security, LAN, WAN, etc. This would involve a review by the Section owner of the key findings and recommendations for each section, and an analysis of the continuing validity of the recommendations. This may require the assistance of a third-party consultant to facilitate and provide additional input. The Sectional review should span a one-month time period to allow for reviewing and making required updates to the associated Sectional elements.

- **Plan Refresh:** The final category of review is a Plan Refresh. This would involve a complete review of the document, including the business drivers and technical vision elements of the plan. Using the current plan as a baseline it would require engaging a third-party consultant to conduct a similar type of analysis as was required in development of the original plan. It is anticipated such a review would span a three-month time period.

With these general categories of evaluation in mind, the following schedule is recommended for Hydro:

Evaluation Category	*6 months*	*12 months*	*18 months*	*24 months*
Directional Review	X		X	
Sectional Review		X		
Plan Refresh				X

The proposed schedule is designed to ensure the document continues to be an integral part of the ongoing IT Management Plan for Hydro.

10.0 Implementation Plan

10.1 Program Overview

The migration towards more wide spread IT solutions has made it necessary to promote more computing standards across dispersed organizations. A Core Technology Infrastructure Program is designed to provide the highway and the connections needed in the areas of mainframe, midrange, networking, and workstations, to support the organization's business model.

The Core Technology Infrastructure Program consists of a number of concurrent and sequential projects designed to provide the organization with the core infrastructure needed to support it's current and future anticipated business solutions. The program supports the long-term business and technical strategies and goals of the organization by establishing the appropriate operating environment for the organization's business systems.

The program, while recommending current technology and stable, reliable and scaleable solutions, is designed to limit or mitigate any negative impact on the dealings of the organization's departments.

The major benefits to be derived from this program are to:

- Make it easier for the organization to do business with itself
- Enhance competitive advantage by enabling the organization's departments to share information.
- Provide a technical leadership example to clients using emerging technologies in a model operating environment

In general, the Core Technology Infrastructure Program consists of the following major activities:

1) Form Management Team and Steering Committee - A Program Team will be formed to develop and manage the Program. A Steering Committee will be established to guide the Program Team and to monitor the program's progress. Reviews will be conducted with the Steering Committee as required.

2) Establish individual project initiatives, schedules, and deliverables.

3) Assign Project Primes who will, under the direction of the Program Manager, be charged with successfully completing their project deliverables for various initiatives.

4) Assign Client Primes to identify the associated business impacts and priorities.

5) Develop resource requirements - Complete estimates of work associated with each project initiative and provide resource requirements and availability for the program.

6) Develop budget - Prepare budget projections for each project initiative, consolidate and provide budget overview for entire program.

7) Finalize roles and responsibilities for all team members and the various departments associated with each project initiative.

8) Acquire necessary funding approval and program approval

9) Manage Program - manage the program's various project initiatives across the organization to provide the project deliverables.

One key ingredient of any Core Technology Infrastructure Program is the Program Charter, which is designed to achieve consensus between the customer and the supplier as to each project's objectives, scope and approach, constraints, and assumptions for the deliverables of the Core Technology initiatives.

The objectives of a Core Technology Infrastructure Program Charter are to:

- Establish a common framework under which the project will proceed;
- Establish a baseline scope against which the project will be managed;
- Put in place mechanisms necessary to manage the project and control its progress;
- Organize, assemble and enable a skilled project team; and,
- Identify project deliverables.

10.2 Approach

Based on the short term recommendations outlined in this report, a series of ten projects have been developed that will form the basis of the Core Technology Infrastructure Program for Hydro. Detailed Project Plans have been included in Appendix D - Project Plans. These plans include a project summary, scope and approach, and deliverables. In addition, selected benefits and risks have been identified where applicable. It is important to note, however, that these are not meant to provide an exhaustive list, but instead to act as a basis for Hydro to develop its own benefits and risks on a per-project basis.

The overall approach to the resulting Program focuses on developing the IT infrastructure in Hydro Place, and then rolling out technology in the field in a coordinated manner as upgrades are scheduled in each location. For technology projects that are more centralized in nature, such as SAN or the Network Management project, the majority of activity is concentrated in the Hydro Place location. The associated Project Timelines are contained in Section 10.3.4.

It is important to note that, while each project has been developed to focus on a single key area, there is a high level of interdependency and scheduling coordination. As a result, it is necessary that Hydro look at the overall Program as a unified whole, and not just as a sum of its individual parts.

10.3 Program Elements

10.3.1 Projects

10.3.1.1 Local Area Network (LAN)

The purpose of this project is to create a reliable, scaleable and manageable LAN/WAN for Hydro utilizing Layer three switching, VLAN and Gigabit Ethernet technologies. Where possible redundant layer three switches and a router redundancy protocol will be utilized to provide redundant inter-VLAN routing. Layer three switching offloads inter-VLAN route processing from the WAN routers, promoting the use of VLANs. Additional VLANS at Hydro will:

- Improve network performance by decreasing the broadcast domain.
- Enhance security when access-lists are implemented between VLANS.

The new network will support aggregate Gigabit Ethernet technology to supply bandwidth scaleable to 16 gigabits.

- Four core switching designs are utilized through-out the Hydro network:
- Fully redundant chassis based layer three switch.
- Dual fixed configuration layer three switch.
- Dual layer two-switched core.
- Layer three switch with integrated T1 WAN interface.

Which of the four designs gets implemented in an area office is mainly dependant on the user count and growth at the location. Hydro Place is getting a chassis based layer three switch at the core with enough Gigabit connectivity to support Gigabit connections to the access layer. Each wiring closet will comprise its own VLAN at this location and an Executive VLAN used to facilitate security. Full redundancy will be achieved in year two by adding redundant supervisors, route processors and line cards to the core switch. Redundant route processors can utilize a router redundancy protocol and provide automatic fail-over capability for inter-VLAN routing. As well the additional Gigabit interfaces at the core will allow for aggregate connections to the access layer, increasing bandwidth and redundancy.

10.3.1.2 Wide Area Network (WAN)

The purpose of this project is to create a reliable, scaleable and manageable, IP protocol based WAN for Hydro.

When complete, the end user will see improved network performance by reducing latency through the increase of usable bandwidth by the integration of internet & and mission critical applications on common facilities. The deployment of T1 cards in routers and increased access speeds will reduce serialization delays.

The project will also provide improved network reliability by implementing ring-based architecture to support major sites where Hydro's private infrastructure & Frame Relay services exist.

10.3.1.3 Internet

The purpose of this project is to create a secure, scaleable and manageable, broadband Internet portal at Hydro Place.

When complete the end user will see improved network performance through the use of full-duplex 10M access and reduced latency of a typical Internet query.

The project will also provide improved network security, as the topology will utilize a dedicated facility thus eliminating risks associated with the shared accesses (e.g. network discovery and multicast-storms).

10.3.1.4 Servers

The purpose of this project is to create a reliable, scaleable and manageable server infrastructure for the Remote Office File/Print and Messaging as well as Functional servers.

The server infrastructure at Hydro is responsible for hosting and maintaining service to the end-user client base, and consists of both core application and network servers housed at Hydro Place, and file/print and messaging servers distributed throughout the WAN. Given the requirement for 99.99% availability for these services it is necessary to have full redundancy and High Availability (HA) clustering configurations for all servers. As with other elements of the network, there must not be any single point of failure in the design. The type and level of HA and redundancy varies depending on the type of server infrastructure in question.

The results of the project include:

- An increase in availability of services through deployment of Microsoft Clustering.
- Hardware upgrades applied to existing servers.
- A replacement of older servers with new models.

10.3.1.5 End User Infrastructure

As indicated in the Project Vision, employees will primarily use electronic methods to communicate within the enterprise, and with this in mind the long-term technical design has significant implications on the way people will complete their job functions in the future. The differences in people's location and job function dictate different approaches to implementing end-user infrastructure.

The purpose of this project is to create a reliable and efficient thin client infrastructure, implementing a combination of thin client appliances and Citrix Metaframe for Support Staff in locations outside St. John's. For support staff much of the interaction with core applications will be dictated by the architecture for each application. Core applications will utilize a three–tier architecture whereby the end-user will interact with the system using a thin client appliance. The specific thin-client architecture will be dictated by the location and function of the support staff.

For those support positions outside St. John's where a significant amount of end-user processing is required, such as conducting financial analysis, or where specialized applications are required, such as Computer Aided Design or Geographic Information Systems, a thin client arrangement using a desktop PC coupled with an application such as Citrix would be used. This would provide the end-user with a combination of local desktop processing power, as well as thin client access to the core applications. As with the server infrastructure, the desktop / laptop configurations would be based on standardized configurations.

10.3.1.6 Security

The security project is designed to address a number of short term recommendations which must be completed to enhance Hydro's overall security. This project must work in conjunction with all other enhancements in place for the network and technologies. The prime areas of security that this project will address include:

- Create an effective Security Policy document
- Plan for the implementation of a single sign-on solution
- Address remote vendor support issues
- Plan for Hydro to conduct routine vulnerability assessments
- Centralized log monitoring and analysis
- Implement Intrusion Detection Systems in key locations

10.3.1.7 Physical Facilities

This project is intended to implement consistent physical facilities to support the networking, communications and server equipment at all Hydro locations. Physical facilities are required to accommodate equipment, as well as supplying suitable levels of power, UPS and air conditioning. Hydro locations and facilities were reviewed and the information was used to develop a standardization plan.

10.3.1.8 Network Management

The purpose of this project is to design and implement a Network Operations Center (NOC) to enable enterprise level management of Hydro's corporate IT systems throughout

Newfoundland according to industry standard IT Service Management model "best practices". The guiding principle of IT Service Management is that IT services are there solely to support the business and its efficient and effective operation. The three main objectives of Service Management are:

- To align IT services with current and future needs of the business and its customers;
- To improve the quality of IT services delivered; and
- To reduce the long term cost of service provision.

The NOC will be the physical nerve center for the equipment and personnel whose primary function is to keep the Newfoundland Hydro corporate systems infrastructure running smoothly. It will be comprised of a team of network, operational and customer support specialists who monitor the IT infrastructure and provide troubleshooting and customer support (i.e. Help Desk) services 24 hours a day, 365 days a year.

10.3.1.9 Storage Area Network (SAN)

The purpose of this project is to provide a fiber channel based Storage Area Network (SAN) for Hydro. This project is a three phase project with data backup & recovery, data storage, and branch/remote office components. The first two phases are to be implemented within the data center at Hydro place. The data backup & recovery phase focuses moving these services to a switched fiber channel fabric and deploying multiple small-mid sized tape libraries. The data storage phase will build upon the existing infrastructure deployed in the previous phase. This phase involves adding redundancy to the fiber fabric and server interconnects, installing central storage enclosures and disk, and moving application data into the SAN. The final phase focuses on deploying SAN technologies in the regional and remote offices. The key criteria in determining whether or not SAN technologies will be deployed in a specific regional/remote office are the existence of cluster technologies.

10.3.1.10 Windows Evolution

Hydro is currently utilizing a single NT Domain on a Windows NT 4.0 Server platform for application and file/print services and Windows NT 4.0 Workstation as a desktop operating system. The goal of this project is to migrate the servers and NT Domain to Windows 2000 Server and Active Directory and the desktops to Windows 2000 Advanced. **xwave** recommends upgrading the servers before the desktops so that Hydro can utilize the desktop deployment features of Windows 2000 and Active Directory. With this in mind, however, it is important that consideration be made of the refresh schedule for the desktop infrastructure and efforts be made to coordinate the project, so as to avoid duplication in upgrades to the end-user infrastructure.

10.3.1.11 Core Applications

The Core Applications Project is unique in that, while a review of the infrastructure supporting the core applications was undertaken, the applications themselves were considered out-of-scope. As was identified in the Technical Report, the core applications infrastructure is largely defined by the application itself, in both its scope and scale. As such, developing detailed design specifications in the absence of a Core Applications Architecture would not prove beneficial.

In order to allow the overall Core Technology program to commence several assumptions were made about the current and future core applications. In designing the IT infrastructure the required flexibility to modify based on changes to the core applications was part of the design criteria. The main assumptions were as follows:

- JD Edwards will continue to be used as the main ERP system for Hydro, and will be based on the use of an AS/400 system in the Hydro Place data center
- The implementation of JD Edwards One World will occur and will require a three-tier architecture using Metaframe
- Lotus Notes will continue to be used for both messaging and as a database application for collaborative data management
- Over time there will be increased integration between JD Edwards, Lotus Notes, and reporting from the Energy Management System

10.3.2 Program Management

It is assumed that the Core Technology Program will be pursued within the ambitious timeframes outlined. These timeframes, and the interdependencies of the projects which comprise the Program, require a significant program and project management effort. The program management effort relates to:

- Coordinating efforts, resources and knowledge across multiple projects;
- Monitoring and managing progress and performance of the Core Technology Program;
- Resolving issues elevated by the project teams;
- Identifying economies of scale in project development, standards, procedures and tools; and,
- Ensuring the Core Technology Program addresses the broader interests of the enterprise.

In addition, the individual projects require a project management effort to:

- Manage risk, issues and changes
- Document and communicate project performance; and
- Manage the quality of the project.

It is assumed that for Years 1, 2 and 3 the combined program and project management will require two (2) full time equivalents of effort (1 FTE = 260 days). This level of project management is in addition to the effort required for delivery of the network management project. For years 4 and 5, it is assumed that 1 full time equivalent of effort will be required.

10.3.3 Key Considerations

This section identifies issues which Hydro must consider prior to commencing any one of the individual projects detailed in this Plan. The nature of information systems is that potential conflicts in project implementation arise, mainly as a result of individual projects which share requirements and components. For example, the implementation of one project could prevent the completion of another project or require considerably more effort, all of which could have been avoided.

The following points illustrate some of the key considerations for Hydro prior to proceeding with the projects identified:

- The horizontal cabling at each site must be category 5e or better tested at 100Mbps and the vertical fiber cabling tested at 1Gbps prior to the LAN upgrade.

- The LAN/WAN modifications and the Windows 2000 server migration could be executed during the same site visit provided both skill sets are present. It is possible in this scenario that problems with the LAN/WAN upgrade will impede the 2000 migration. The scheduling conflicts would be most prevalent at sites getting new servers because the LAN/WAN may be required during server configuration and data migration.

- Server and desktop hardware must meet (preferably exceed) Microsoft's minimum hardware recommendations.

- Minimum of 1.5 Megabits of bandwidth required between sites prior to the VoIP trial

- WAN management visibility required before VoIP trial and the integration of mission critical applications and the Internet traffic.

- QoS application evaluation required before VoIP trial and the integration of mission critical applications, Internet traffic and the Citrix thin client deployment.

- Bandwidth upgrades required before Citrix thin client is deployed.

- Do not perform the Windows 2000 migration and the Windows 2000 Clustering during the same site visit. This approach allows the network to stabilize and aids the trouble-shooting process by limiting the scope.

- Windows 2000 Advanced Server is noted as the Operating System for the Server Clusters. As newer OSs are introduced by Microsoft, the Operating System may change. For example, in Years 3,4,and 5 the OS may not be Windows 2000 but rather a follow on product.

- The Server Clustering project is dependent upon the timelines for the Windows 2000 Migration Project. A delay in that project may delay this project's timelines

- The Thin Client project is dependent upon the timelines for the Windows 2000 Migration Project since Citrix Metaframe XP is based upon Windows 2000. A delay in that project may delay this project's timelines.

- The proposed Thin Client solution is focused on remote sites only. Implementation at Hydro Place would require additional costs and effort.

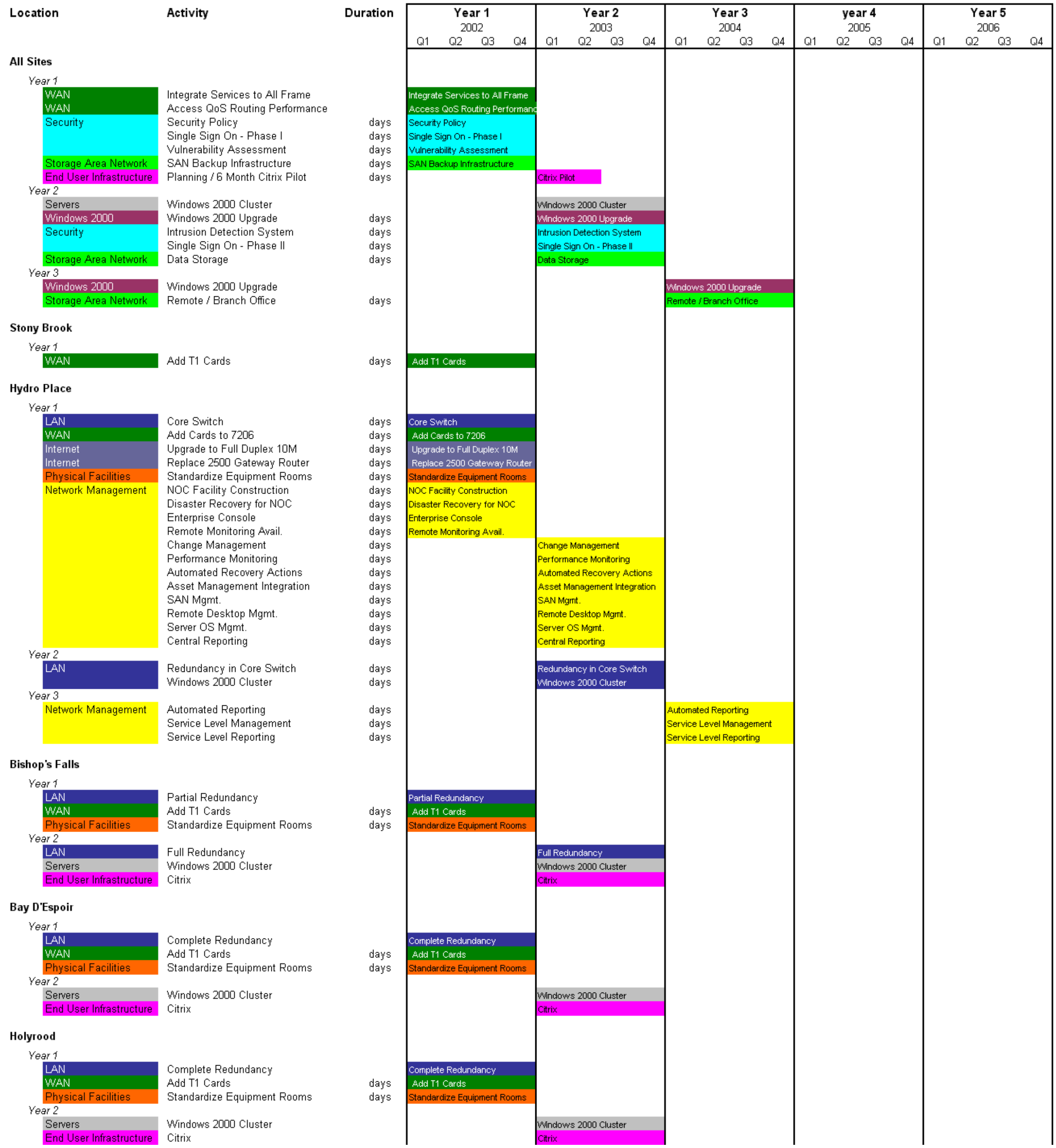
- Hardware and software implementations must be coordinated between team members to ensure completion during the initial setup and configuration of all network and server devices.

- All implementation team members must have access to Hydro environment and facilities (i.e. swipe cards, pass codes) to ensure easy flow of movement throughout various sites.

10.3.4 Project Timelines (Gantt Chart)

HYDRO
THE POWER OF COMMITMENT

Newfoundland Hydro
Infrastructure Assessment
Core Technology Plan
Gantt Chart



Location	Activity	Duration	Year 1 2002	Year 2 2003	Year 3 2004	year 4 2005	Year 5 2006
			Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4
All Sites							
Year 1							
WAN	Integrate Services to All Frame		Integrate Services to All Frame				
WAN	Access QoS Routing Performance		Access QoS Routing Performanc				
Security	Security Policy	days	Security Policy				
	Single Sign On - Phase I	days	Single Sign On - Phase I				
	Vulnerability Assessment	days	Vulnerability Assessment				
Storage Area Network	SAN Backup Infrastructure	days	SAN Backup Infrastructure				
End User Infrastructure	Planning / 6 Month Citrix Pilot	days		Citrix Pilot			
Year 2							
Servers	Windows 2000 Cluster			Windows 2000 Cluster			
Windows 2000	Windows 2000 Upgrade	days		Windows 2000 Upgrade			
Security	Intrusion Detection System	days		Intrusion Detection System			
	Single Sign On - Phase II	days		Single Sign On - Phase II			
Storage Area Network	Data Storage	days		Data Storage			
Year 3							
Windows 2000	Windows 2000 Upgrade				Windows 2000 Upgrade		
Storage Area Network	Remote / Branch Office	days			Remote / Branch Office		
Stony Brook							
Year 1							
WAN	Add T1 Cards	days	Add T1 Cards				
Hydro Place							
Year 1							
LAN	Core Switch	days	Core Switch				
WAN	Add Cards to 7206	days	Add Cards to 7206				
Internet	Upgrade to Full Duplex 10M	days	Upgrade to Full Duplex 10M				
Internet	Replace 2500 Gateway Router	days	Replace 2500 Gateway Router				
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Network Management	NOC Facility Construction	days	NOC Facility Construction				
	Disaster Recovery for NOC	days	Disaster Recovery for NOC				
	Enterprise Console	days	Enterprise Console				
	Remote Monitoring Avail.	days	Remote Monitoring Avail.				
	Change Management	days		Change Management			
	Performance Monitoring	days		Performance Monitoring			
	Automated Recovery Actions	days		Automated Recovery Actions			
	Asset Management Integration	days		Asset Management Integration			
	SAN Mgmt.	days		SAN Mgmt.			
	Remote Desktop Mgmt.	days		Remote Desktop Mgmt.			
	Server OS Mgmt.	days		Server OS Mgmt.			
	Central Reporting	days		Central Reporting			
Year 2							
LAN	Redundancy in Core Switch	days		Redundancy in Core Switch			
	Windows 2000 Cluster	days		Windows 2000 Cluster			
Year 3							
Network Management	Automated Reporting	days			Automated Reporting		
	Service Level Management	days			Service Level Management		
	Service Level Reporting	days			Service Level Reporting		
Bishop's Falls							
Year 1							
LAN	Partial Redundancy		Partial Redundancy				
WAN	Add T1 Cards	days	Add T1 Cards				
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 2							
LAN	Full Redundancy			Full Redundancy			
Servers	Windows 2000 Cluster			Windows 2000 Cluster			
End User Infrastructure	Citrix			Citrix			
Bay D'Espoir							
Year 1							
LAN	Complete Redundancy		Complete Redundancy				
WAN	Add T1 Cards	days	Add T1 Cards				
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 2							
Servers	Windows 2000 Cluster			Windows 2000 Cluster			
End User Infrastructure	Citrix			Citrix			
Holyrood							
Year 1							
LAN	Complete Redundancy		Complete Redundancy				
WAN	Add T1 Cards	days	Add T1 Cards				
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 2							
Servers	Windows 2000 Cluster			Windows 2000 Cluster			
End User Infrastructure	Citrix			Citrix			

Newfoundland Hydro

Infrastructure Assessment

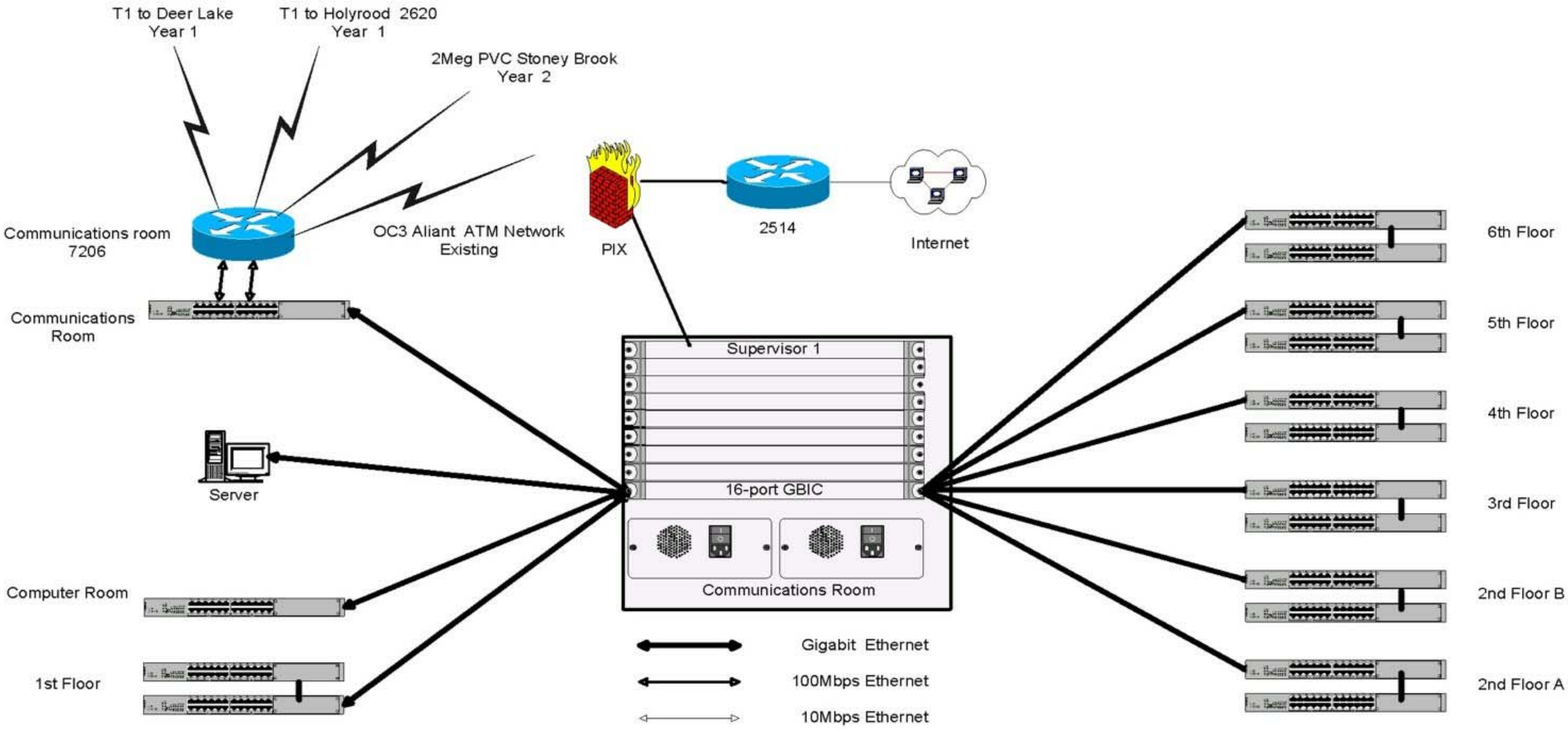
Core Technology Plan

Gantt Chart

Location	Activity	Duration	Year 1	Year 2	Year 3	year 4	Year 5
			2002	2003	2004	2005	2006
			Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4	Q1 Q2 Q3 Q4
Churchill Falls							
Year 1							
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 2							
LAN	Partial Redundancy			Partial Redundancy			
WAN	Add T1 Cards	days		Add T1 Cards			
Servers	Windows 2000 Cluster			Windows 2000 Cluster			
End User Infrastructure	Citrix			Citrix			
Year 3							
LAN	Full Redundancy				Full Redundancy		
Deer Lake							
Year 1							
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 2							
LAN	Complete Redundancy			Complete Redundancy			
WAN	Install 4224	days		Install 4224			
Servers	Windows 2000 Cluster			Windows 2000 Cluster			
End User Infrastructure	Citrix			Citrix			
Port Saunders							
Year 1							
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 3							
LAN	Complete Redundancy				Complete Redundancy		
WAN	Install 4224	days			Install 4224		
Servers	Windows 2000 Cluster				Windows 2000 Cluster		
End User Infrastructure	Citrix				Citrix		
St. Anthony							
Year 1							
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 3							
LAN	Complete Redundancy				Complete Redundancy		
WAN	Install 4224	days			Install 4224		
Servers	Windows 2000 Cluster				Windows 2000 Cluster		
End User Infrastructure	Citrix				Citrix		
Stephenville							
Year 1							
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 4							
LAN	Complete Redundancy					Complete Redundancy	
WAN	Install 4224	days				Install 4224	
Servers	Windows 2000 Cluster					Windows 2000 Cluster	
End User Infrastructure	Citrix					Citrix	
Happy Valley - Goose Bay							
Year 1							
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 4							
LAN	Complete Redundancy					Complete Redundancy	
WAN	Install 4224	days				Install 4224	
Servers	Windows 2000 Cluster					Windows 2000 Cluster	
End User Infrastructure	Citrix					Citrix	
Wabush							
Year 1							
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 5							
LAN	Complete Redundancy						Complete Redundancy
WAN	Install 4224	days					Install 4224
Servers	Windows 2000 Cluster						Windows 2000 Cluster
End User Infrastructure	Citrix						Citrix
Whitbourne							
Year 1							
Physical Facilities	Standardize Equipment Rooms	days	Standardize Equipment Rooms				
Year 5							
LAN	Complete Redundancy						Complete Redundancy
WAN	Install 4224	days					Install 4224
Servers	Windows 2000 Cluster						Windows 2000 Cluster
End User Infrastructure	Citrix						Citrix

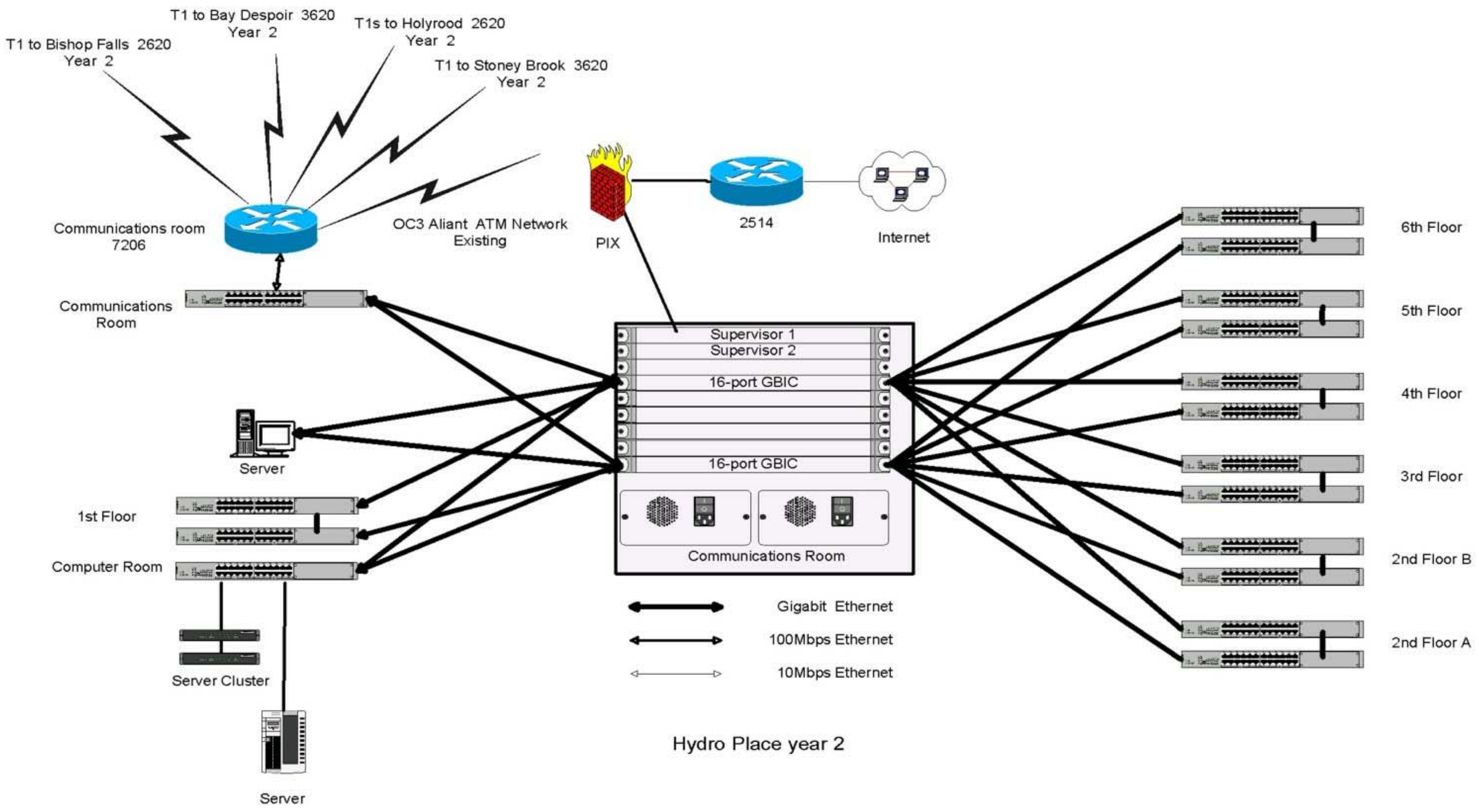
10.3.5 Diagrams

10.3.5.1 Hydro Place - Year 1



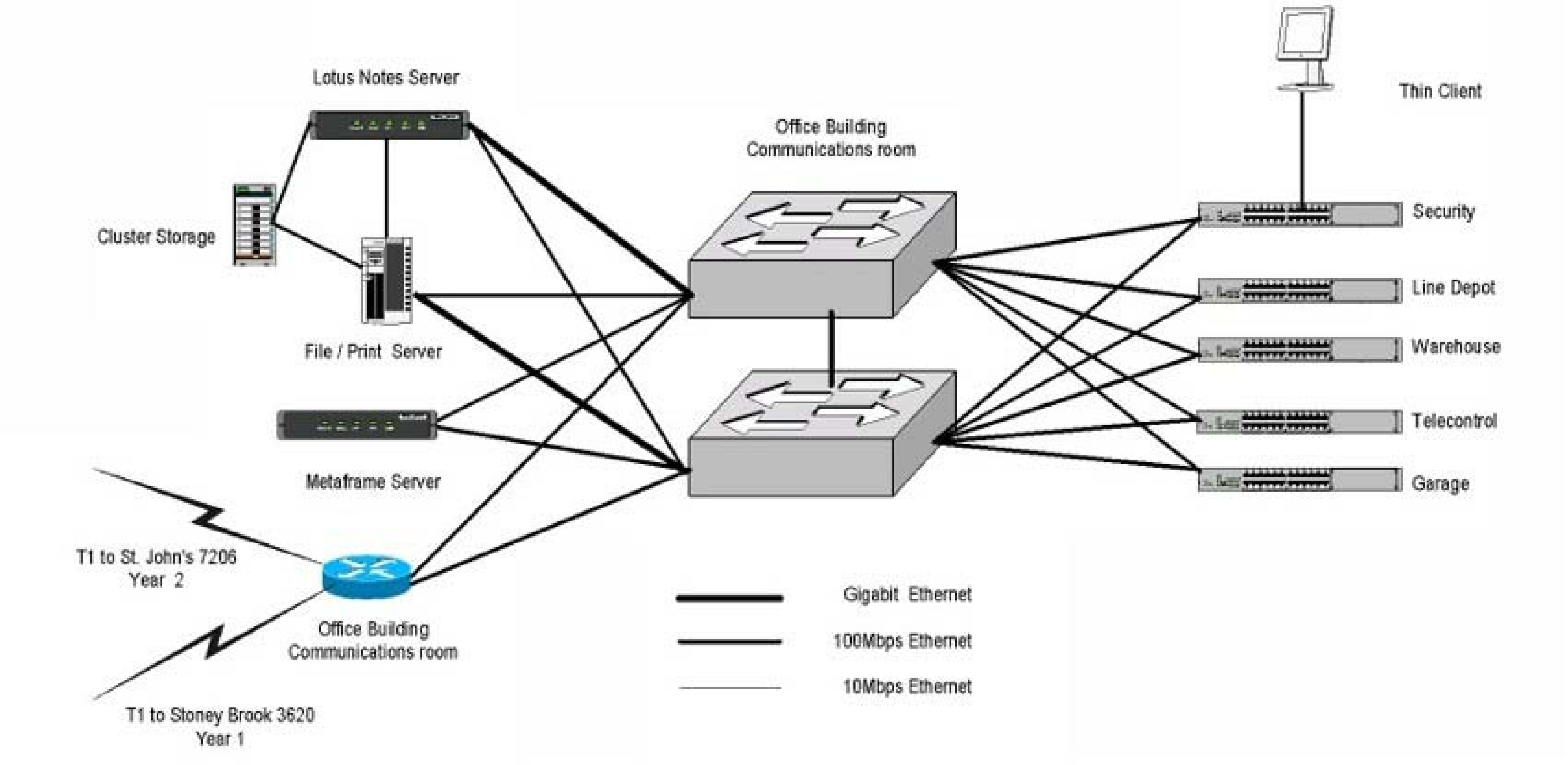
Hydro Place year 1

10.3.5.2 Hydro Place - Year 2

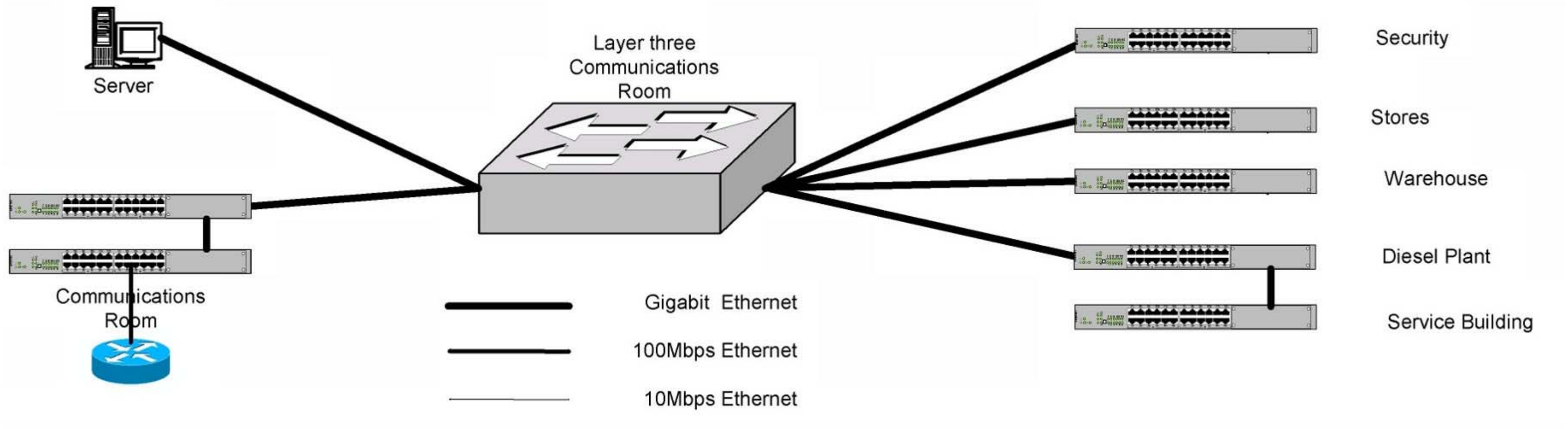


Hydro Place year 2

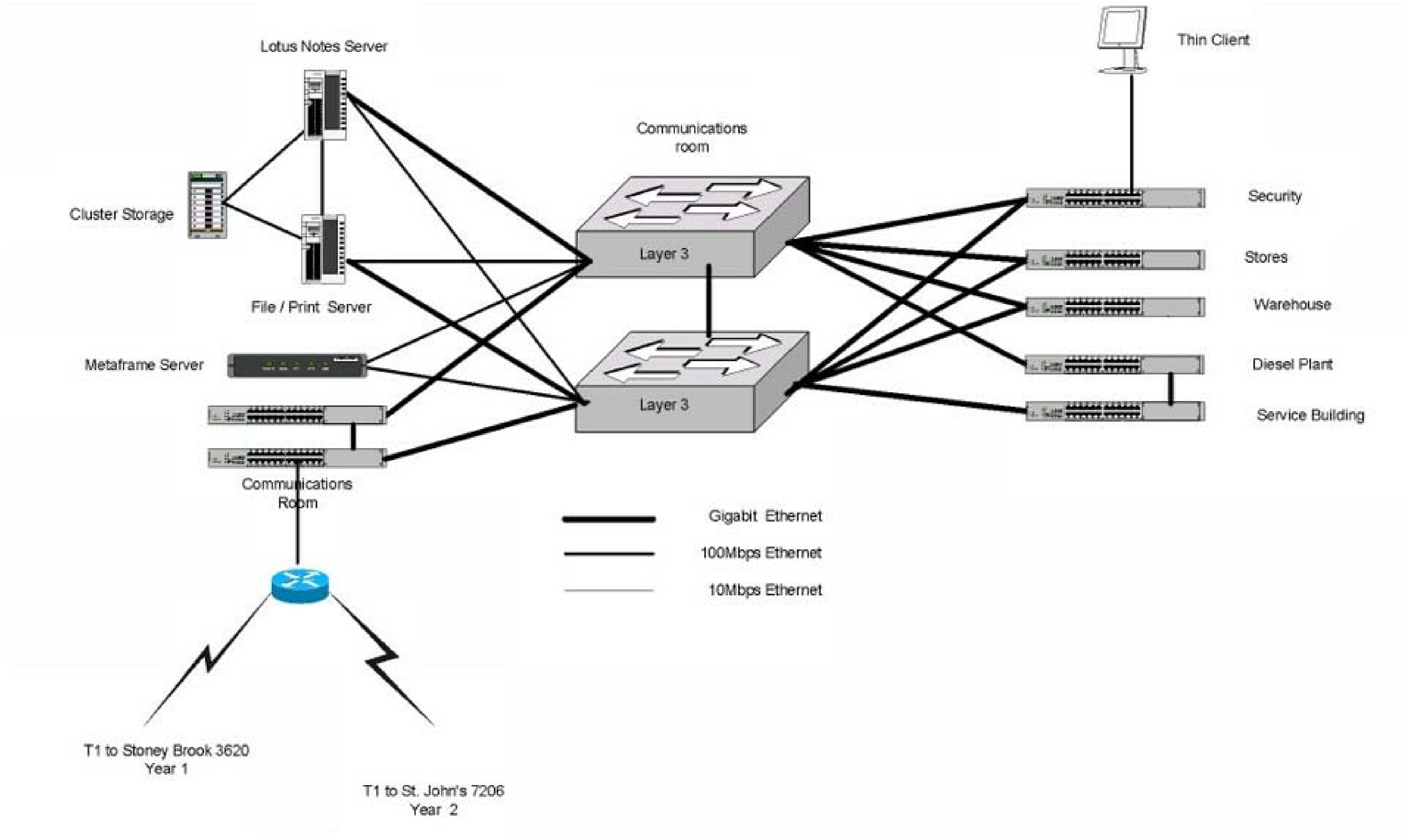
10.3.5.3 Bay D'Espoir - Year 1



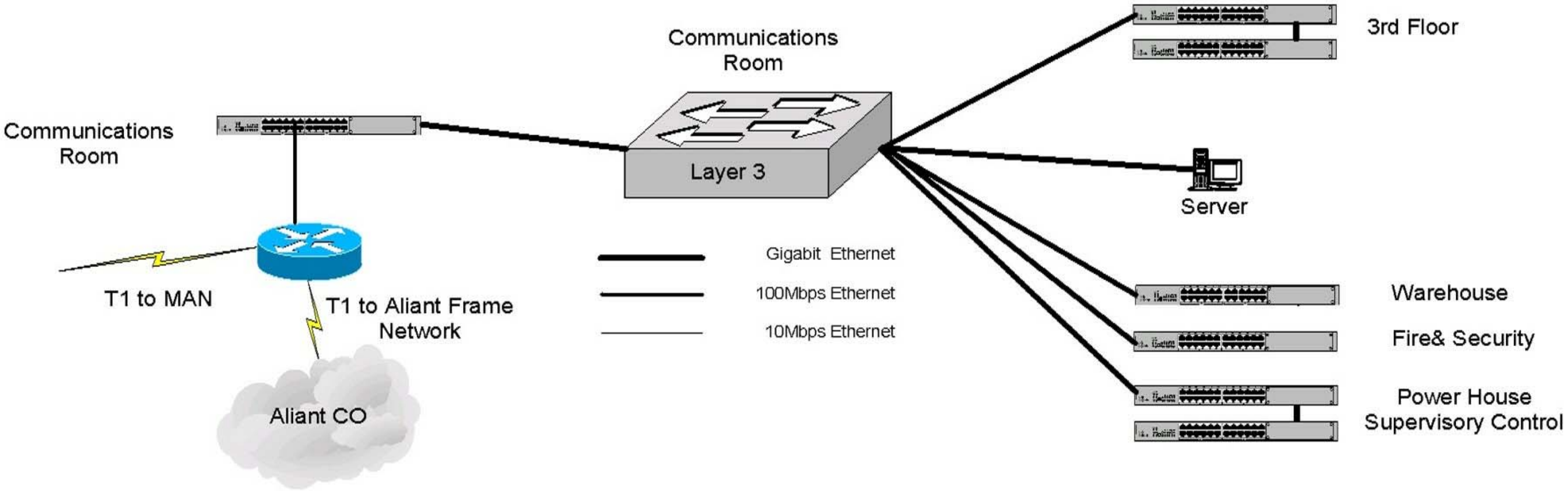
10.3.5.4 Bishop's Falls - Year 1



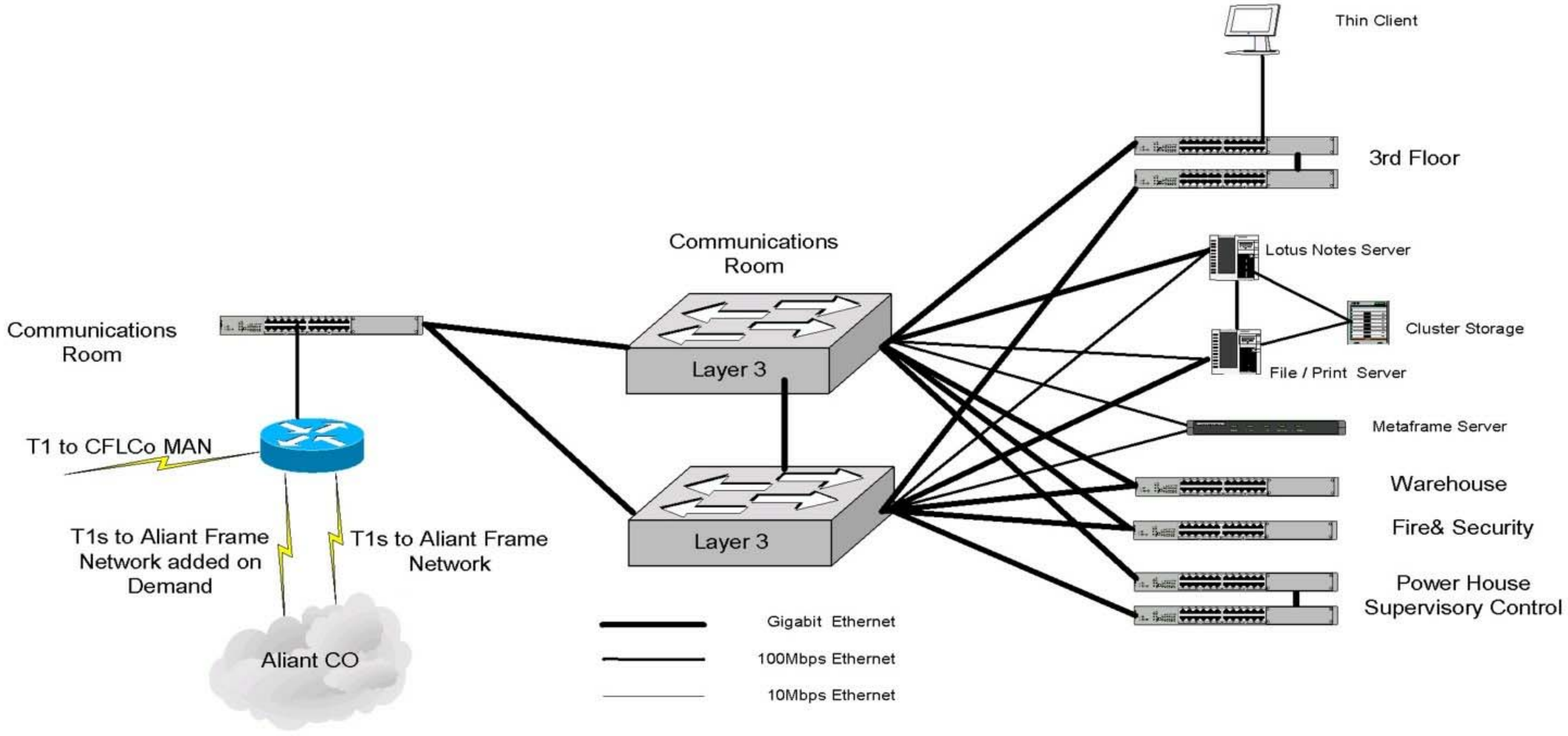
10.3.5.5 Bishop's Falls - Year 2



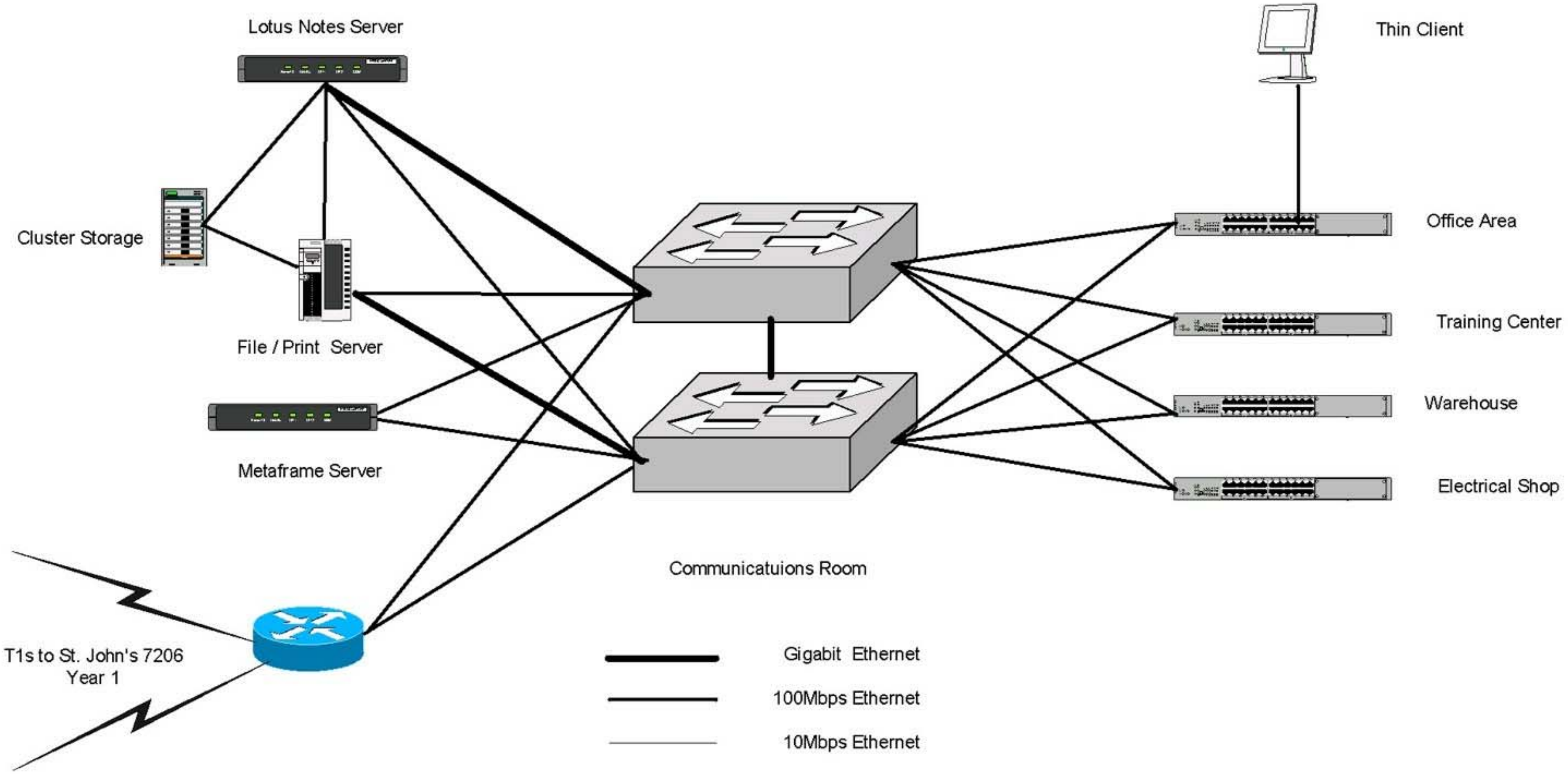
10.3.5.6 Churchill Falls - Year 2



10.3.5.7 Churchill Falls - Year 3

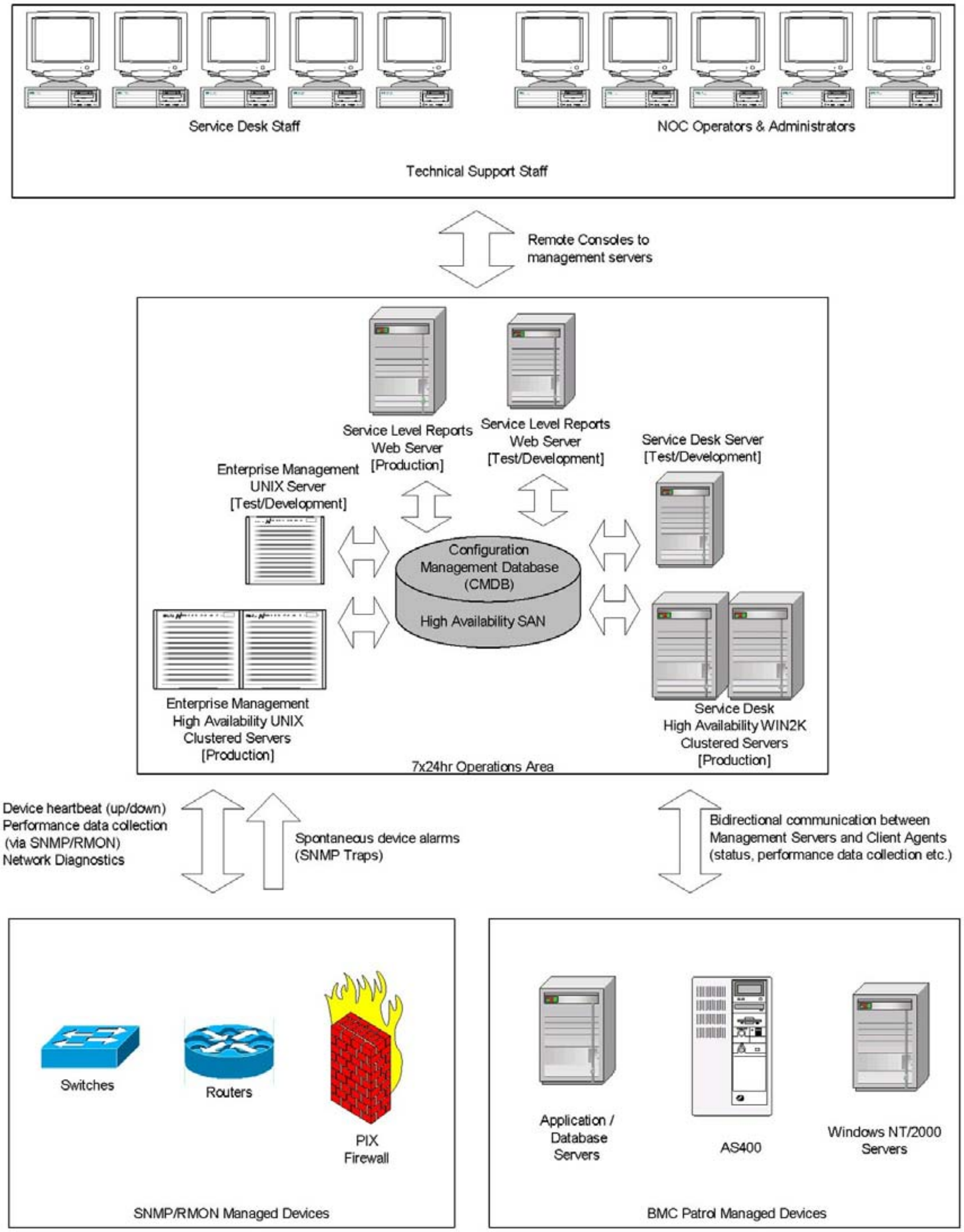


10.3.5.8 Holyrood - Year 1



10.3.5.9 Network Management

Network Management Plan - Appendix 1 - NOC Conceptual Diagram


Service Desk Staff
NOC Operators & Administrators
Technical Support Staff
Remote Consoles to management servers
Service Level Reports Web Server [Production]
Service Level Reports Web Server [Test/Development]
Service Desk Server [Test/Development]
Enterprise Management UNIX Server [Test/Development]
Configuration Management Database (CMDB)
High Availability SAN
Enterprise Management High Availability UNIX Clustered Servers [Production]
Service Desk High Availability WIN2K Clustered Servers [Production]
7x24hr Operations Area
- Device heartbeat (up/down)
- Performance data collection (via SNMP/RMON)
- Network Diagnostics
Spontaneous device alarms (SNMP Traps)
Bidirectional communication between Management Servers and Client Agents (status, performance data collection etc.)
Switches
Routers
PIX Firewall
SNMP/RMON Managed Devices
Application / Database Servers
AS400
Windows NT/2000 Servers
BMC Patrol Managed Devices

11.0 Glossary

Term **Definition**

ARP (Address Resolution Protocol) A method for finding a host's Ethernet address from its Internet address. An ARP request is sent to the network, naming the IP address; then the machine with that IP address returns its physical address so it can receive the transmission.

ATM (Asynchronous Transfer Mode) A network technology that enables the transmission of data, voice, audio, video, and frame relay traffic in real time.

Bridge A device that governs the flow of traffic between networks or network segments and forwards packets between them.

CIDR (Classless Inter-Domain Routing) A method for more efficient use of the existing 32-bit Internet Address Space.

CoS (Class of Service) A way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, large document file transfer) together and treating each type as a class with its own level of service priority. Unlike Quality of Service (QoS) traffic management, Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time.

DCHP (Dynamic Host Configuration Protocol) Windows NT Server software that assigns an IP address to each node in a network.

DNS (Domain Name System) A database system that translates an IP address into a domain name. For example, a numeric address like 232.452.120.54 can become something like xyz.com.

DoS Attack Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

DSU/CSU (Digital Service Unit/Channel Service Unit) A way of connecting a communications line to an external digital circuit.

EIGRP (Enhanced Interior Gateway Routing Protocol) A network protocol that lets routers exchange information more efficiently than with earlier network protocols.

ERP (Enterprise Resource Planning) The planning and management of all the resources in an enterprise. Also refers to a multi-module software system that supports enterprise resource planning. An ERP system typically includes a relational database and applications for managing purchasing, inventory, personnel, customer service, shipping, financial planning, and other important aspects of the business.

Ethernet
The most popular type of local area network, which sends its communications through radio frequency signals carried by a coaxial cable. Each computer checks to see if another computer is transmitting and waits its turn to transmit. If two computers accidentally transmit at the same time and their messages collide, they wait and send again in turn.

gBIT
One billion bits.

GBPS
Gigabits per second (billion bits per second).

GDC-OCM
A product of General Data Comm., OCM (Office Communications Manager) platforms offer connectivity to a variety of digital carrier services, allowing users to select the one with the best performance/cost ratio in each location. They use the same bandwidth optimization techniques as the TMS-3000 to efficiently transport voice and data traffic.

GDC-TMS
A product of General Data Comm., GDC TMS class products provide an advanced internetworking platform that offer bandwidth management for high-speed wide area networks. The Multi-nodal, Multi-aggregate architecture of the product enables service providers and enterprise users to build fully mesh, fault tolerant resilient backbone networks.

IDS
(Intrusion Detection System) Inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

IGRP
(Internet Gateway Routing Protocol) A proprietary interior gateway protocol used to exchange routing information between Cisco Systems routers.

IP
(Internet Protocol) The IP part of TCP/IP; the protocol that is used to route a data packet from its source to its destination over the Internet.

ISP
(Internet Service Provider) A company that provides Internet accounts.

LAN
(Local Area Network) A network that connects computers that are close to each other, usually in the same building, linked by a cable.

MAN
(Metropolitan Area Network) A network that serves a metropolitan area. Compare LAN and WAN.

mBIT
(Mb, mbit or Mbit) 1,048,576 bits, or 1024 kilobits. A measurement of the capacity of memory chips. Also used to mean one million bits.

MUX (Multiplexer) A hardware device that enables two or more signals to be transmitted over the same circuit at the same time by temporarily combining them into a single signal.

NAT Short for Network Address Translation, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

NOC (Network Operations Center) A center that monitors a network and communicates with other networks on the Internet, to improve services and solve problems.

PDC (Primary Domain Controller) Primary domain controller (PDC) and backup domain controller (BDC) are roles that can be assigned to a server in a network of computers that use the Windows NT operating system. Windows NT uses the idea of a domain to manage access to a set of network resources (applications, printers, and so forth) for a group of users.

Proxy Server A server that provides access to files from other servers by retrieving them either from its local cache or from the remote server.

QoS (Quality of Service) A term which specifies a guaranteed throughput level. One of the biggest advantages of ATM over competing technologies such as Frame Relay and Fast Ethernet, is that it supports QoS levels. This allows ATM providers to guarantee to their customers that end-to-end latency will not exceed a specified level.

RAID (Redundant Arrays of Independent Disks) The use of two or more disk drives instead of one disk, which provides better disk performance, error recovery, and fault tolerance, and includes interleaved storage techniques and mirroring of important data.

RAS Short for Remote Access Services, a feature built into Windows NT that enables users to log into an NT-based LAN using a modem, X.25 connection or WAN link.

Router A device that finds the best path for a data packet to be sent from one network to another.A router stores and forwards electronic messages between networks, first determining all possible paths to the destination address and then picking the most expedient route, based on the traffic load and the number of hops.

SAN (Storage Area Network) A high-speed network that connects multiple storage devices so that they may be accessed on all servers in LAN or WAN.

SCADA Acronym for Supervisory Control and Data Acquisition, a computer system for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation

SNMP (Simple Network Management Protocol) The Internet standard protocol for network management software. Using SNMP, programs called agents monitor various devices on the network (hubs, routers, bridges, etc.).

T1 A telephone line connection for digital transmission that can handle 24 voice or data channels at 64 kilobits per second, over two twisted pair wires.

TCP/IP The Transmission Control Protocol (TCP) on top of the Internet Protocol (IP).These protocols were developed by DARPA to enable communication between different types of computers and computer networks. The Internet Protocol is a connectionless protocol which provides packet routing. TCP is connection-oriented and provides reliable communication and multiplexing.

TDM (Time Division Multiplexing) A multiplexing technique (a way of transmitting two or more signals at the same time over the same communications channel) in which the individual signals are combined by interleaving bits. This technique is used with T-1 carriers in wide area networks.

Token Ring A local area network in which computers are configured in a ring, and a message called a token is passed from station to station. The token is used to avoid conflicts in transmission; a machine can only transmit messages while it holds the token.

UPS (Uninterruptible Power Supply) A backup power supply that works when electrical power to the computer is interrupted.

UTP Unshielded Twisted Pair. The cable used for most telephone wire, and is also used for some computer-to-computer communications.

VLAN Short for virtual LAN, a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

VoIP (Voice over IP) A term used for a set of facilities for managing the delivery of voice information using the Internet Protocol (IP). In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN).

VPN (Virtual Private Networking) A means by which certain authorized individuals (such as remote employees) have secure access to an organization's intranet by means of an extranet (a part of the internal network that is accessible via the Internet).

WAN (Wide Area Network) A network in which computers are connected to each other over a long distance, using telephone lines and satellite communications. Contrast with Local Area Network (LAN).

WINS (Windows Internet Naming Service) A program that runs under Windows NT Server which correlates the host name of a computer on a network with its physical IP address, thus making it possible to find computers on other networks.

Appendix A

Business Needs Research Interview Guides

Newfoundland and Labrador Hydro
Information Systems Integration Strategy

Business Needs Analysis
Executive Interview Guide

AN ALIANT COMPANY

Interview Objectives

1. Understand the business direction & strategy
   - And, what is required of IT to support the business and its strategy.

2. Understand how senior management uses information to run the business.
   - Is the available information meeting your needs? If not, what are the issues, gaps and opportunities?
   - Are there other more general issues regarding Information Technology that should be considered or discussed here?

HYDRO

Overview of Future Direction/Corporate Strategy

- What is Hydro’s future direction and where will this lead the organization over the next five years?
- How will this direction impact:
  - New lines of business (telecom, engineering services)
  - Focus on retail vs wholesale power distribution
  - Partnerships (e.g. wind generation initiatives)
  - The Employer/Employee relationship (attracting skilled workers into remote job sites, work trends such as telework, replacing an aging workforce, etc)

xwave
AN ALIANT COMPANY

Discussion of Key Business Drivers

- What are Hydro's key business drivers?
  - Stakeholders
    - Hydro Internal (Employees)
    - Hydro External (Government, General Public)
  - Regulatory Environment (e.g. PUB)
  - Demands for high quality, timely information (internal & external)
  - Customer Expectations and Requirements
  - Environmental Issues
  - Financial & Economic factors (internal & external)

- How must Hydro respond to these?
- Given constraints facing Hydro, how well is the organization positioned to effectively respond?
- Are there gaps that need to be addressed?
- How can IT help address these gaps?

Critical Success Factors

- What are the **key** things that Hydro must do in order to be successful; to meet its goals and objectives?

- What is the role of IT in supporting Hydro reaching these objectives?

Opportunities -

- What are the most significant opportunities that Hydro may be positioned to take advantage of or capitalize on?
  - From your perspective, is Hydro positioned to take advantage of the opportunities?
  - If not, what gaps need to be addressed?
- What role do you see for Information Technology in helping Hydro capitalize on these opportunities?

Threats -

- What are the most serious threats facing Hydro and what can be done to eliminate or mitigate these?
  - From your perspective, is Hydro positioned to address identified threats?
  - If not, what gaps need to be addressed?
- What role do you see for Information Technology in helping Hydro address these threats?

Management Information Needs

- In general, what are your information requirements?
  - Current
  - Future state
- What Key Performance Indicators do you rely on?
- Are there issues or opportunities with respect to KPI or related information?
- Are there issues or opportunities with respect to specific applications and their ability to provide the information required to run the business?
- Are there other more general issues or opportunities with the data and information that you use?
  - Ownership
  - Quality
  - Timeliness
  - Relevancy
- What role do you see for Information Technology in supporting Hydro’s information requirements?
  - Comment on the Strategic vs. Tactical role for IT
- Are there other ways to leverage the investment Hydro has made in IT?

Issues around the Hydro Organization Structure

- Hydro is a geographically dispersed organization. Given this, what are the key interdependencies between operating units and/or offices in the Hydro group of companies?
- What are the issues and and challenges involved with “tying the organization together”.
  - How does IT assist or hinder in this view?
- What’s working and what isn’t?

Other Issues for Discussion

- e.g. What are your most immediate/pressing needs with respect to IT?

Glossary of Terms

Business Driver – Factor that leads the organization efforts.

AN ALIANT COMPANY

Newfoundland & Labrador Hydro

Business Unit Interview Guide

1) A description of your Department

- How is your Department organized and where are employees located?
- What is your Department's mandate, its main functions, responsibilities and objectives?
- How does your Department relate to other Hydro Departments? (internal)
- How does your Department relate to other Hydro stakeholders? (external)

2) Information Requirements in support of your Mandate

- What are the information needs of your Department? Are they currently being met? If not, what are the gaps?
- What are the sources of information that you use (both internal and external sources)?
- Is the information that you receive readily useable? If not, what do you have to do to make it useful to you and your staff?
- How is the information used by your Department?
- What Key Performance or other Management Indicators are used to help you manage?
- Does the available information support KPI well? If not what are the issues?
- How would you rate the ability of you and your staff to access the information that is required?

  What are the issues, gaps and challenges?
  Are there issues with ownership, timeliness, accuracy and /or relevancy of information?

3) Achieving your Mandate and Objectives

What are some of the key challenges faced by you and your group in achieving your objectives?

What support do you require from the organization to be effective and to achieve your objectives (e.g. staff, sufficient authority, etc?

What are the general issues, challenges and gaps here?

Is Information Technology effective in supporting your ability to attain your objectives?

If not, what can/must IT do in future to support you better?

What are the main processes and / or functions that you conduct in your Department? Where does the information (data) come from that drives these operations?

Are there key processes or functions in your operation that must change in order for you to achieve your objectives or to align with changes in the organization?

What are they and how can IT support this transformation?

If you could provide an example of a "success story" from your Department that might be duplicated in other areas to enhance the effectiveness of the organization, what would that be?

4) Hydro's 5 Year Strategic Direction

What is your understanding of the key elements of Hydro's business vision and direction?

From your perspective, what are the key strategic issues and success factors that must be addressed or realized by Hydro to achieve its goals?

What role does your Department play in helping achieve the overall strategic direction of the organization?

With respect to change caused by implementing the organizational strategy, what will your Department have to do to prepare for and support such changes?

What support do you require from the organization to assist you in this regard?

What IT support do you require to assist you in this regard?

Appendix B

Employee Survey

Definitions

Corporate Network – This is the computer network operated by the company that allows people to share files, get e-mail and have access to various computer systems operated for the company. To access the Corporate network you must use a Username and Password.

Personalized Home Page – Some Internet sites allow users to customize the information they receive through "personalization". With a personalized site you receive information such as sports scores for your favourite teams, or financial information on stocks you may own.

Network Resources – Some computer programs are located on your office computer, while others use the Corporate Network to provide information to your computer. As an example, when you use Microsoft Word the computer loads the program from your local hard drive, but when you use Lotus Notes a small program on your computer (called a "client") talks to the main Lotus Notes program located on a large computer on the Corporate Network.

Home Technology Use

1. In considering your own familiarity with computers, would you say you are a:

   a. Non-user,
   b. Beginner,
   c. Intermediate, or
   d. Expert

2. Do you currently have a Personal Computer at home?

   a. Yes
   b. No

3. Do you currently have Internet access at home?

   a. No ***go to question 4***
   b. Yes, via my own Dial Up connection ***go to question 5***
   c. Yes, via my own High Speed connection (ex: Sympatico Warp, RoadRunner. Satellite, etc.) ***go to question5***
   d. Yes, through dial up to the Corporate network ***go to question 5***

4. Which of the following is the **most important** reason why you do not have Internet access at home?

   a. I don't have a computer at home
   b. I don't see the value
   c. I don't have time to use the Internet at home
   d. It's too difficult to use
   e. Other (specify)

Office Technology Use

5. What type of computer do you use in your office location?

a. No computer ***go to question 41***
b. Desktop PC
c. Laptop
d. Both Desktop and Laptop

6. Do you currently have Internet access at work?

a. No ***go to question 9***
b. Yes, via the Corporate network
c. Yes, via Dial Up connection

7. Which of the following job-related activities do you engage in when you access the Internet from work? *Check all that apply*

a. Accessing user groups / communities
b. Purchasing
c. Training
d. Research
e. Technical Support
f. Other (specify)

8. Have you ever "Personalized" a home page using tools available on a web site, such as Sympatico or Yahoo?

a. Yes
b. No
c. Unsure

Corporate Network

9. In the past month, how frequently have you connected to the Corporate network from your primary work location?

a. Not At All ***go to question 41***
b. > 10 times
c. between 10 and 20 times
d. > 20 times

10. In the past month, approximately how many times have you connected to the Corporate network from another office or from home?

a. Not At All
b. 1 to 2 times
c. 3 to 10 times
d. > 10 times

Please indicate on a scale from 1 to 5 where 1 is "strongly agree" and 5 is "strongly disagree" how strongly you agree or disagree with each of the following statements:

11. The time it takes for my computer to access information from the network does not inhibit me in completing my job.

12. I find the speed and response time of the Corporate network acceptable

13. There are times when I want to get access to information on the Network, but the application or network isn't available.

Software Application Use

14. When you access your office computer, which of the following programs do you use regularly? *Check all that apply*

a. Microsoft Word
b. Microsoft Excel
c. Microsoft Access
d. Microsoft PowerPoint
e. Internet Explorer
f. Lotus Notes
g. Microsoft Project
h. Computer Aided Design (CAD) software
i. Visio
j. Adobe Acrobat
k. Other (specify)

15. When you access the Company network, which of the following resources do you use regularly? *Check all that apply*

a. E-mail (Lotus Notes)
b. Internet Access
c. JD Edwards
d. Strategy Showcase
e. Harris Energy Management System
f. Lotus Notes Databases
g. Shared File Space (Common Drives)
h. NetMeeting
i. Other (specify)

Please indicate on a scale from 1 to 5 where 1 is "strongly agree" and 5 is "strongly disagree" how strongly you agree or disagree with each of the following statements:

16. When I get data from JD Edwards, I usually end up having to do my own changes using a program on my desktop/laptop computer to provide the information I need.

17. I find JD Edwards provides me with all the functionality I require to complete my job.

18. I find JD Edwards difficult to use.

19. JD Edwards provides me with the necessary information to complete my job.

20. Using Strategy / Showcase is an easy way to get the information I require.

21. I believe implementing JD Edwards was a worthwhile investment by the Company.

22. I prefer to use my own desktop tools (Office Suite, MS Project, etc.) to conduct my work, and then put the information back into JD Edwards.

23. I have received an appropriate level of training to use JD Edwards effectively.

24. I have received an appropriate level of training to use the Microsoft Office Suite provided with my Office computer.

25. I have received an appropriate level of training to use Lotus Notes effectively.

26. I find it difficult to read documents, such as e-mail or reports, on my computer screen and usually print them off to review.

27. I try to keep a paper copy of information in a file for safe-keeping and/or easy access.

Technical Support

28. How frequently in the past month have you called the Helpdesk?

a. Not At All ***go to question 30***
b. 1 to 3 time
c. 4 to 6 times
d. > 6 times

29. For which of the following reasons have you contacted the Helpdesk in the past month? *Check all that apply*

a. E-mail support
b. Desktop application support
c. Hardware / equipment failure
d. Unable to access the network
e. Slow response from the network
f. Unable to access information in JD Edwards
g. Unable to access information in a Lotus Notes Database
h. Forgot / reset password
i. Printer support
j. Other (specify)

30. In the past three months have you used any type of online support function available on the Internet? (i.e. Microsoft's Support site, etc.)

a. Yes
b. No
c. Unsure

31. In the past month have you used the “Help” option (or “F1” key) in an application to try and solve a problem or learn how to complete at task?

a. Yes
b. No
c. Unsure

Please indicate on a scale from 1 to 5 where 1 is “strongly agree” and 5 is “strongly disagree” how strongly you agree or disagree with each of the following statements:

32. When I contact the Helpdesk I find they respond to my request in a timely manner.

33. When I contact the Helpdesk I find they are able to provide appropriate responses to my issues.

34. As compared to twelve months ago, I have seen an improvement in the performance of the Helpdesk function.

35. I would prefer to access training material on software applications over the Company network on my own schedule.

36. I would prefer to receive training on software applications delivered in a classroom or workshop setting.

Security

Please indicate on a scale from 1 to 5 where 1 is “strongly agree” and 5 is “strongly disagree” how strongly you agree or disagree with each of the following statements:

37. There are so many computer passwords for me to remember that I use a system or write them down.

38. I do not find the password security keeps me from being able to do my work efficiently.

39. I do not have the access privileges to get information I need to complete my work.

40. Given the sensitive nature of the Company’s information, I believe the security systems in place to protect data are appropriate

41. If the Company was to provide each office with a computer terminal any employee could use to connect to the company network, would you be very likely, likely, unlikely or very unlikely to use the facility at least once per month?

a. Very Likely
b. Likely
c. Unlikely
d. Very Unlikely

Demographics

42. Which of the following best describes your general job function?

a. Executive / Director / Manager
b. Professional (Engineering, Accounting, IT, etc.)
c. Front Line Supervisor
d. Clerical
e. Maintenance
f. Other (specify)

43. In which of the following locations are you primarily based?

a. St. John’s
b. Holyrood
c. Whitbourne
d. Happy Valley
e. Wabush
f. Stephenville
g. Deer Lake
h. St. Anthony
i. Port Saunders
j. Churchill Falls
k. Bay D’Espoir
l. Bishops Falls

44. In which of the following Divisions are you currently employed?

a. Transmission and Rural Operations
b. Finance
c. Production
d. Human Resources and Legal
e. CF(L) Co.

45. Into which of the following general ranges does your total length of service with the Company fall?

a. < 5 years
b. 5 to 10 years
c. 11 to 15 years
d. 16 to 20 years
e. 21 to 25 years
f. > 25 years

46. Are you:

  a. Male
  b. Female

Are there any comments you would like to make about this survey, or about Hydro's use of Information Technology?

Appendix C

Technical Survey Questionnaire

1 Infrastructure Assessment

1.1 Server

1.1.1 Function	Is the server functionally an enterprise or workgroup server?	
	What is the server's primary function?	
1.1.2 Configuration	Who is the manufacturer (Sun, IBM, HP, etc)?	
	What is the model?	
	When was it purchased?	
	What are the component parts?	
1.1.3 Software	**Operating System**	
	What is the operating system?	
	What is the software version and patch level?	
	Do you monitor any services or applications on the server (e.g. Oracle instances, Internet Services, Microsoft Exchange)?	
	Do you use any network management tools to manage the server?	
	Applications	
	What software is installed (database, mail, backup, batch scheduling)?	

	What is the software version and patch level?	
	Version Control Process	
	Describe version control environment / toolsets. Are tools like Microsoft SMS used?	
	Is there a schedule for upgrading software?	
	Is there usually an outage experienced during the upgrade? How long?	
	What is the procedure for identifying and implementing new updates and versions?	
	Who identifies the need for updates and upgrades?	
	Who approves the updates and upgrades?	
	What is the procedure for communicating to the client's information about upcoming updates and upgrades?	
1.1.4 Capacity	**Disc storage**	
	How much disc space is in the server?	
	How many disc drives are in the server?	
	What types of disc drives?	
	What is the speed of the drives (Ex: 10K RPM)?	
	How are the discs configured?	

	What is the expansion capability of the disks?	
	Memory	
	How much memory is in the server?	
	How is the memory configured (e.g. 8X256MB DIMMS)?	
	What is the expansion capability for memory?	
	Processing Power	
	How many CPUs are in the server?	
	What is the type of CPU (e.g. Xeon, PII)?	
	What is the speed of the CPUs?	
	What is the expansion capability for CPU's?	
1.1.5 Availability	**High Availability Configurations**	
	Is High Availability software/hardware running on the server (e.g. Sun Clustering, IBM HACMP)?	
	How long does it take for the server and application to be up and running again after a failure?	
	What is the version of the software? Does the vendor support the installed version?	
	Has there been a controlled HA software tested?	
	Fail Over Procedures	
	What procedures are in place in the event of a failure (e.g. notifications, backup retrieval, client signoff)?	

	Are the procedures documented?	
	Have the Fail over procedures been tested?	
1.1.6 **Technical Support**	**Support Contracts and SLA’s**	
	Who is responsible for initiating support contracts for equipment and software?	
	Who makes sure that the contracts are maintained yearly?	
	Are contracts for resources costed as fixed or as time and labor?	
	Are SLA’s developed for production applications?	
	Who is responsible for developing SLA’s?	
	Do the technical support resources provide input to the SLA’s (e.g. input to availability and performance commitments)?	
	What are the areas covered in the SLA’s (e.g. Availability, Performance)?	
	What is the usual duration of an SLA?	
	Change management procedures	
	Do Change Management processes currently exist (e.g. notifications, change windows)? If so, are they documented?	
	Describe the current restrictions / controls as relating to the timing of installations of new hardware/software within the environment.	
1.1.7 **Redundancy**	**Software Redundancy**	
	How is this achieved (e.g. mirroring, RAID-5,)?	

Options	If so, what data and how (e.g. OS, Apps)?	
	Hardware Redundancy	
	How is this achieved (mirroring, RAID-5,)?	
	Does the server have redundant power supplies, fans, controllers, network cards, etc?	
1.1.8 Storage Requirements	**Backup and Restore requirements and policies**	
	What is the current tape management method (e.g. DLT, DAT, ArcServe)?	
	Is the process manual or automated?	
	What are the current policies for data archiving and backups (e.g. frequency, duration a backup is kept)?	
	Does a separate backup network exist?	
	Are backups being stored at a separate site?	
	Disaster Recovery processes	
	Describe the disaster recovery procedures in place for the server and applications running in it.	
	Have the disaster recovery procedures been tested?	
	Is there a regular schedule for testing (Ex: semiannually)?	
	Storage Area Networks / Network Attached Storage	
	Does the server use external disk arrays?	
	Does the server make use of any SAN's?	

1 Infrastructure Assessment

1.2 Desktop

1.2.1 Standard Configuration	**Standard Configuration**	
	Who is the manufacturer (e.g., IBM, HP)?	
	What is the model?	
	What are the component parts?	
	What is the operating system?	
	What is the software version and patch level?	
	What software is installed (e.g., MS Office, Lotus Notes Mail and Databases, Visio, JD Edwards, Client Access400)?	
	What are the software versions and patch levels?	
	Version Control Process	
	Describe version control environment / toolsets. Are tools like Microsoft SMS used?	
	Is there a schedule for upgrading software?	
	What is the procedure for identifying and implementing new updates and versions?	
	Who identifies the need for updates and upgrades?	
	Who approves the updates and upgrades?	
	Capacity	
	How much disc space is in the desktop/laptop?	
	How much memory is in the desktop/laptop?	
	How is the memory configured (e.g., 2X64MB DIMMS)?	
	What is the type of CPU (e.g., PII)?	
	What is the speed of the CPU?	

<table>
<tr><th colspan="3">1.2a Non-Standard Computing Devices</th></tr>
<tr><td><b>1.2.2 Non-Standard Devices</b></td><td>Please identify the type and function of non-standard computing devices that connect to the corporate network (such as meter reading devices, etc.), and</td><td></td></tr>
<tr><td></td><td>Where are these devices located? Describe how they interact with the network.</td><td></td></tr>
<tr><td></td><td>Which applications do they interface with?</td><td></td></tr>
</table>

1 Infrastructure Assessment		
1.3 Printer		
1.3.1 Configuration	**Standard Configuration**	
	Who is the manufacturer (e.g., IBM, HP, etc)?	
	What is the model?	
	Where is the printer located (site, location within site)?	
	What are the main applications that output to the printer (e.g. JD Edwards reporting, user desktop file print)?	
	What software is installed (e.g., Jetform)?	
	What are the software versions and patch levels?	
	Can the printer print duplex?	
	Is the printer able to produce colour print?	
	Is the printer LAN attached?	
	Is the printer IP addressable?	
	Version Control Process	
	What is the procedure for identifying and implementing new updates and versions?	
	Who identifies the need for updates and upgrades?	
	Who approves the updates and upgrades?	
	Capacity	
	How much memory is in the printer?	
	How is the memory configured (e.g., 2X16MB DIMMS)?	
	What is the speed of the printer (e.g. 20 pages/minute)?	
	How much paper can be stored within the printer?	

1 Infrastructure Assessment

1.4 Data Centre / Equipment Closet Environment s

1.4.1 General	Describe the general style of building containing the data centre (e.g., Purpose built or evolved centre, wood frame/ wooden walls, steel frame/ wooden walls, steel frame/ concrete walls)	
	Who owns and manages the building?	
	Where is the building located?	
	Are there clear markings or branding to distinguish the data centre from the rest of the building?	
	Is the data centre wheelchair accessible?	
	Does the data centre have a raised floor?	
	Is the data centre approaching / beyond full capacity?	
	Does the data centre have contiguous space to accommodate anticipated growth?	
	Does a detailed floor plan exist for the data centre?	
	How much server space is required for the foreseeable future?	
	How much space is required for networking and communications equipment?	
	How much space is required for enterprise equipment such as SAN and Data Management?	
	Are there any equipment staging areas available (e.g., test labs)?	
	Is there operations and support staff office space available in the data centre?	

1.4.2 Power Requirements	What is the number of feeds to building?	
	What is the electrical capacity currently available?	
	Describe the in-building electrical distribution systems?	
	What is the capacity, current load in Amps?	
	Is there a single or dual distribution system?	
	If dual, what is the capacity available on each distribution system?	
1.4.3 UPS	What is the current UPS KVA rating?	
	What is the currently UPS steady state power draw?	
	What is the peak UPS power draw?	
	What is the % UPS utilization (e.g., Once UPS usage exceeds 60% it is usually scheduled for upgrade. A UPS utilisation over 80% is considered unacceptable in a data centre environment)?	
	Where is the UPS located?	
	What is the number of hours of UPS battery backup required?	
1.4.4 Fire Suppression	What are the current fire suppression method and capabilities (e.g., chemical, gas system, wet-pipe sprinkler system, dry-pipe, pre-action system with high-temperature heads, two stage systems)?	
	Are pipes within the system welded together, or merely clamped?	
	Are there racks with permeable doors and cages with wire walls to enable rapid access to the source of fire without the delays of obtaining rack or cage keys?	
	Is there a standby switch to abort firing of the system?	

	Are there heat sensors and smoke sensors existing and adequate?	
	How many extinguishers are available to supplement the primary fire suppression system?	
1.4.5 Air Conditioning	Describe the existing HVAC equipment (e.g., make, manufacturer)?	
	What is the HVAC capacity rating in tons?	
	Is there redundancy for HVAC systems?	
	Is there an existing load shedding protocol (e.g., when and in what order to turn off monitors and equipment in data centre)	
	Are there HVAC system and humidity monitors?	
	Describe failure mode for HVAC. (e.g., open/full blast)	
	Does separate venting for the data centre than for the broader building exist?	
	Is all air conditioning on the same UPS power system as the rest of the data centre?	
1.4.6 Wiring / Cabling	What are the procedures for installing and maintaining wiring / cabling?	
	Is the ability to trace a problem hard or easy?	
	Is the power wiring secured and isolated from data?	
	Is the network wiring secured?	
	Is there a possibility for server outage while people are working around the servers and communications equipment (e.g., tripping over cables, pushing restart buttons inadvertently)?	

	Is there available equipment storage (open shelving, retrofitted racks, purpose built racks / proprietary cabinets)?	
1.4.7 Racking	Does the data centre use racks to house servers?	
	When equipment is ordered, does it arrive rack ready?	

2 Processing Design

2.1.1 Module	What is the module name?	
	What is the version and patch level? Is this the latest version available from the vendor?	
	What is the primary function of the module?	
	From what other modules or applications does this module receive data? In what form?	
	To what other modules or applications does this module provide data? In what form?	
	Which departments / functional groups have data entry access to this module?	
	Which departments / function groups have data read access to this module?	
	When was the module installed?	
2.1.2 Hardware	On what server(s) does this module reside?	

	Which server(s) does this module access in its processing function (i.e. database servers, apps servers, replication servers, web servers, etc.)?	
2.1.3 Client	Do end-users directly interface with this module? If so, is it through a custom client or browser interface?	
	What is the software version and patch level for clients?	
	What is the recommended computing platform for the client?	
	How are client changes managed and deployed (SMS, site visits, etc.)	
2.1.4 Dependant Data Flows	What data flows from this module to either end users or other modules?	
	Where does this data reside? What is the version and patch level of the database?	
	What is the approximate volume of data transferred (in GB)	
2.1.5 Availability	Are there any availability restrictions on this module? If so, please identify.	

	When and how frequently are data backups conducted? How does this impact on availability of the module?	
	What systems are used for conducting backups? Who is the primary owner of the systems?	
	Please outline the data restore process.	
	Is the module available during batch processing (read only, update)?	
2.1.6 Business Owner	Who is the business process owner for this module?	
	Please outline the change management process for this module.	
	Where is the documentation for this module maintained? Who is the owner of the documentation	

3 Local Area Network Design

3.1 Desktop

3.1.1 IP subnet design	Do all desktops have an IP address?	
	Are the IP addresses in use internet-registered?	
	Who maintains the IP registry of assigned addresses?	
	What domain names are registered?	
	What DNS is authoritative for these domain names?	
	What IP address ranges are assigned for your usage?	
	Are all servers referred to by IP address or a WINS/DNS host name? If not, how are they named?	
3.1.2	Provide a copy of all network diagrams available for the Server Farm/Room and Client workstations.	
	Describe the network infrastructure (routers, switches, managed elements).	
	Is there a separate network environment for Production and Development services?	
	Describe connection speeds of and interfaces to (Ethernet or token ring) the Hydro LAN.	
	Describe network protocols other than IP, i.e. SNA or NETBIOS in use on LANs and WANs.	
	Comment on the cabling infrastructure, is it CAT 5 or less? Are there plans to re-wire in the near future?	
	Describe the use of VLANS in the current network.	
	What type of remote access environment is in use (RAS, Cisco Access Servers, etc)?	

	Are there applications in use at your environment that put heavy demands on network bandwidth? What are they? Describe any Remote Access hardware and software and document the RAS application requirements.	
	Is your internal company network connected to the Internet?	
	Describe your thin-client environment if used.	
	What type of mainframe connectivity do you support i.e. client access, Twinax?	
1.4.8		
3.1.3 **Server infrastructure**	**Name servers DNS/WINS**	
	What DNS technologies are in use at your location i.e. NT , UNIX?	
	Do you have a primary, and secondary DNS? Do you use Caching DNS for internal name resolution?	
	Do you maintain static name resolution files i.e. LMHOSTS or HOSTS files on individual servers?	
	DHCP servers	
	Are DHCP assigned addresses updated on the DNS infrastructure (Dynamic DNS)? Do you have redundant DHCP server scopes for key areas?	
3.1.4 **Management software**	See Toolset section in **Network Management Design**	

3.1.5 **Testing, monitoring & measurement tools**	See Toolset and Monitoring Requirements sections in **Network Management Design**	

4 Wide Area Network Design

4.1 General

4.1.1 Applications	List all applications that use the WAN and the servers on which these the applications reside.	
	Provide the IP addresses for each server	
	Provide the number of users on an application perspective at each remote office	
4.1.2 Routers	Provide hardware inventory for all routers in NF Hydro's network. Include all makes, models, ports, network modules & WICs on a per site basis.	
	Provide copy of running configuration of each router. Provide the software IOS feature set and release level for each router.	
	Is there a support contract in place for the routers? If so, provide details.	
4.1.3 Circuits	Provide a listing of all privately own circuits supporting the NF Hydro WAN. Include the location of the terminal points (from a machine to machine basis), the applications residing on each circuit and the bandwidth supported on each circuit.	
	Provide any copies of any WAN documentation and drawings that may be applicable.	
	Provide detail on the terminal locations and the provisioned capacity of the existing microwave radios supporting the WAN.	

	Provide detail on the radio networks planned for future WAN support, including initial capacity to be provisioned & their total capacity.	
	Provide a copy of the network performance study complete using the Concord platform.	
4.1.4 Mulitplexors	Provide hardware inventory for all multiplexors in NF Hydro's network. Include all makes, models, low speed ports, and aggregate modules on a per site basis.	
	Configuration - provide detail on how each MUX is configured such that circuit routes & available bandwidth are described.	
4.1.5 Network Evaluation	Identify high end users on an application basis to be used during the network measurement phase of the evaluation.	
	Identify trouble applications with high response times at the specific users with the problem to be reviewed during the network performance measurement activity.	

4.1.6 **Network Performance**	Provide ping latency measurements at three periods of a typical day on per circuit basis (Remote router to St. John’s Router) at the following times of the day: Busy hour, Typical normal traffic condition, And after hours	
	Provide response times per application per circuit basis (Remote client to St. John’s Server application) at the following times of the day: Busy hour, Typical normal traffic condition, And after hours.	
4.1.7 **Traffic Optimization**	Provide the file sizes (e.g. batch, mail, ftp) that are being transferred over the WAN. Provide information on when these files are transferred, e.g. during normal business hours & the acceptable time to transfer them.	
	Provide a list of all voice trunks and the bandwidth they consume.	
4.1.8 **Protocols**	Provide detail on all protocols that utilize the WAN	
	Does all WAN traffic use TCP/IP for transport?	
	Are there any other WAN protocols in use (IPX or NetBEUI)?	
	If so for what applications and servers?	
	Provide a description of the WAN traffic flow on an application basis.	
	Are all servers referred to by IP address or a WINS/DNS host name? If not, how are they named?	
	Provide the IP addresses of each server.	

5 Network Management Design

5.1 General

5.1.1 **Toolsets**	Do you employ any framework toolsets for Enterprise Management (e.g., HP Openview, Tivoli, BMC)?	
	Describe the hardware used for Network Management. If a server or workstation is used, please reference the device from the section 1.	
	What network management tools are used for monitoring Hubs? What events are monitored?	
	What network management tools are used for monitoring Switches? What events are monitored?	
	What network management tools are used for monitoring Routers? What events are monitored?	
	What network management tools are used for monitoring Modem Pools? What events are monitored?	
	What network management tools are used for monitoring Servers? What events are monitored?	
	What network management tools are used for monitoring UPS's? What events are monitored?	
	What network management tools are used for monitoring any other miscellaneous devices? What events are monitored?	

	What network management tools are used for monitoring voice traffic? What events are monitored?	
	What network management tools are used for monitoring WAN traffic? What events are monitored?	
	Describe how you monitor any services at the application level. (e.g. Oracle instances, Internet services, Voice and Data applications, etc.)	
5.1.2 Monitoring Requirements	Do all network management alarms and notifications roll-up to a centralized console?	
	How is support staff notified of alarms (e.g. automatic paging, email, Remedy, phone calls)?	
	Please describe procedures used in responding to alarms.	
	Do support staff have remote access to the network to trouble-shoot alarms and notifications?	
5.1.3 Reporting	Describe the reports generated on the health and welfare of hardware and operating system. (e.g. Server availability, CPU, memory and disk utilization)	
	Describe the reports used for monitoring application software. (e.g. Internet services,)	
	Describe how reports are used to proactively support devices and applications.	
	Describe how reports are used in capacity planning and performance tuning.	

6 Security Audit

6.1 Computer Rooms / Physical Building Security

6.1.1 Physical Access	Are all perimeter doors equipped with strong and effective locks, ensuring the absence of vulnerabilities including external door hinges?	
	Are all perimeter windows on the ground level barred, shuttered, grilled or alarmed?	
	Are fire escape entrances properly secured?	
	Are elevators equipped with electronic card readers for after-hours access?	
	Are stairwell doors locked after-hours and are they kept closed?	
	Are all additional points of entry (skylights, roof hatches, manholes, exhaust fans and air conditioning vulnerabilities) properly secured?	
	Is data center area access authority vested in the data centre operator?	
	Describe the in-building data centre access control method?	
	Do loading docks have control processes in place to ensure that access from the dock area to the inner areas of the building is maintained in a secure manner?	

6.1.2 Physical Access Monitoring	Do cameras monitor the outside of the facility as well as the entrances to the data center areas on a 7x24 basis and is camera activity monitored, taped and reviewed? Are the tapes retained for at least 6-8 weeks?	
	Is an alarm system in place for sites that are not manned on a 24*7 basis that is monitored by a private or public response agency?	
	If yes to b, is this system tested on a periodic basis, at least yearly?	
	Is privileged access to the alarm system strictly restricted to only personnel responsible for maintaining building security?	
	Is a security guard force in place with documented processes and procedures?	
	Is the security guard force required to perform rounds throughout the complex and indicating completion of these duties through the use of a wand/check point system?	
6.1.3 Employee Access	Are employees required to show proper company identification (badge with ID) to gain entrance to the building and is employee identification visible at all times?	
	Do all employees enter and exit the facility via a secured access point and is this access monitored by the camera system?	
	Does access system record entrance and exit times in an audit trail that is retained and reviewed regularly?	
	If no to above questions, describe the method whereby access to the building is controlled	

	Are background checks (criminal, drug, prior employment, etc) conducted on employees prior to hire?	
	Is inspection of incoming and outgoing packages (e.g., bags, briefcases, boxes) conducted on a random basis?	
6.1.4 Visitor Access	Are all visitors on a daily basis required to be identified in a log which documents name, organization, person or location visited, time in and time out?	
	Are visitors required to wear badges?	
	Is a badge process in place to ensure that badges cannot be retained in an unauthorized manner?	
	Are documented procedures and tracking in place for approving access requests to secured/restricted areas of the building?	
	Who has frequent visitor access (e.g., consulting groups, companies)?	
	Are visitors required to have an escort at all times when accessing secure areas of the facility such as a computer room?	
6.1.5 Physical Access to Network Resources	Are network drops in empty or infrequently used offices disabled when not in use?	
	Is port based security enabled on equipment that supports this feature to ensure that only the registered secure MAC address belonging to the user assigned to that port access to the LAN?	
	Are wiring closets and other distribution points properly secured?	
	Is physical access to core networking equipment ports restricted to network administrators only?	

	Are audits of activated network ports conducted on a regular basis to ensure that unused ports are not available?	
	Are all user requests for connectivity to LAN resources validated and are the user authorization forms kept?	
	Are laptop computers physically secured to an immovable object when left unattended?	
	Is the use of palm pilots for the storage of corporate data allowed or prohibited?	
6.2 Policies and Procedures		
6.2.1 Security Policies and Procedures	Are Security Policies and Procedures in place that address at a high level; prevention detection, response, disaster recovery, and business continuity?	
	Are there underlying standard operating procedures and configuration guidelines (standard Windows NT workstation configuration for example) to support the high-level security policies?	
	Are the security policies and procedures defined, documented, and distributed to all employees?	
	Are all personnel required to attend an annual security awareness briefing?	
6.2.2 Media Handling	Is access to the tape backup systems and the process of removing tapes from storage areas restricted to authorized personnel only?	
	Is a disposition strategy in place and documented which includes sensitive trash and electronic media?	
	Are sensitive hardcopy data such as network diagrams and configuration information stored in a secure manner and disposed of through shredding when no longer required?	

	Are hard drives wiped with low-level formats or magnetic destruction before disposal, resale, or warranty replacement?	
6.2.3 **Authentication and Authorization**	Do all systems present a logon banner, which states the users responsibilities regarding misuse and access to information on the system, and that information systems access is subject to monitoring?	
	Are cryptic passwords with a minimum length required for access to IT resources on the local LAN and WAN?	
	Are users limited to three unsuccessful logon attempts with a 24-hour period?	
	Are all users assigned a unique system ID for computing system access?	
	Are wireless devices such as PDAs required to have password protection?	
	When informed that a user has transferred, changed job responsibilities, terminated or taken a leave of absence, is their User ID revoked or have their permissions revised immediately?	
	Are automated login scripts and other automated access programs written such that they do not contain unprotected passwords?	
	Do operating systems and applications prevent the local caching of access passwords?	
	Are users permitted to log onto the network from more than one machine at a time?	
	Are users required to power down, log off or lock their computers before leaving for the day?	

	Are screen savers with a minimum time to activation of 10 minutes or less required to be activated on user computers and servers?	
	Are power-on passwords activated for mobile user machines such as laptops?	
	Is the ability to log-on locally disabled for ordinary users?	
	Are all guest and anonymous accounts disabled by default, instead granting specific anonymous permissions only when required?	
	Do you provide ADSL/ISDN/Cable Modem Support for executive or employee remote access?	
	Does dial-in or remote VPN access require the use of password and token authentication (e.g. Strong positive authentication such as SecurID or Digital Certificates)?	
	Are access-lists (authorization) imposed on users upon successful dial-in authentication that limits their access to only required resources and services?	
	If no to above, please describe the authentication method in place for remote access connections.	
	Are access-lists (authorization) imposed on users upon successful dial-in authentication that limits their access to only required resources and services?	
	Is dial-up access limited to centralized communication servers or modem pools?	
	Are modems connected to computers disabled for auto answer mode?	
	Are dial-in servers configured to disable dial-out functions?	

	Is dial-in activity regularly monitored through the use of an automated system or is manual review of logon events used?	
6.2.4 Applications and File Systems	Are all files protected by default from unauthorized access, modification, and deletion?	
	Are system default authorizations that are delivered initially with each system reviewed and removed as required?	
	Are network file system shares available for all users?	
	Are the following rights restricted based on job function and not assigned to users in general? • Restore files and directories • Manage auditing and the security log • Add workstations to a Domain • Take ownership of files or objects • Shutdown the system • Force a shutdown from a remote system.	
	Have application installations and deployment been performed through the use of best practices for security as identified by the vendors of these applications?	
	Has JD Edwards provided guidelines to Hydro for using their applications securely and effectively?	
	Has Lotus provided guidelines for securing the Lotus Notes suite of applications?	
	Have custom applications developed by Hydro or specifically for Hydro been reviewed and inspected by an application security consulting company?	

6.2.5 Network and Functional Boundaries	Are firewalls used for defined network boundaries between Hydro and other partner organizations as well as the Internet?	
	If yes to above, what types of firewall technologies are employed at each location? Please submit vendor and software version as well as information detailing current vendor support entitlements.	
	What other software if any is installed on the firewalls (e.g., Floodgate-1, SSH, etc)?	
	Are firewalls or router access lists used to limit the exposure of systems such as databases that do not need to accept direct user connections?	
	For all edge devices, are only the minimum required network services allowed to traverse the gateway in both directions?	
	Are security policies that are enforced on edge devices reviewed periodically to reconfirm their validity?	
	Can xwave perform a review of the current security rules being enforced on edge devices?	
	Is authentication and authorization enforced at edge boundary gateways wherever possible, limiting the use of host based access-lists?	
	Are direct connections to the Internet or remote domains through the use of DSL or modem strictly prohibited while connected to the LAN?	
	Is network topology or other information available to the outside through the use of DNS reverse lookup zones?	
	Is a minimum of Internal topology information registered with Internic?	

6.2.6 Internet Services	Are network-connected hosts and applications made available to users on the Internet and are these hosts protected by a firewall?	
	Are network-connected hosts that provide applications to users on the Internet separated from the Internal network through the use of a firewall? (e.g. Do these servers reside in a demilitarized zone?)	
	Do any of the firewalls in use force the use of Network Address Translation to hide internal network ranges from destinations on the Internet?	
	Are there hosts on-site outside the Internet firewall?	
	Is inbound and/or outbound FTP allowed?	
	Is inbound Telnet access allowed?	
	If Web services are allowed inbound, is SSL used to transport confidential or sensitive data between the client Web browser and Web Server?	
	Is any sensitive data allowed to remain intact for a definitive time period greater than a few minutes on a publicly addressed host	
	Have vulnerability assessments and service port scans been performed against all public IP addressed hosts (including hosts that are made available through the use of static network address translation) within the last 6 months?	
	Are VPN technologies used and if so, please identify remote offices and number of users connected to Hydro HQ through the use of VPN?	

	If yes to above, is VPN utilizing at least DES encryption strength used for client-to-site or site-to-site connectivity over the Internet?	
	Is encryption used to move confidential or sensitive data over the Internet in all cases?	
	Is remote administration of Internet accessible, publicly addressed hosts allowed from the Internet without strong positive authentication and encryption?	
6.2.7 Vulnerabilities, Viruses, and Trojans	Is anti-virus software of a minimum acceptable standard deployed on all network attached workstations and servers?	
	Are SMTP transmissions scanned for viruses at the edge through the use of SMTP gateway software before entering and leaving the corporate network?	
	Are HTTP and FTP downloads permitted to user workstations and if so, are these downloads scanned for malicious content either at the Internet gateway or at the user's machine?	
	Are software patches that address vulnerabilities reviewed, tested and applied to all workstations and servers when made available by the vendor of the software?	
	Is a process in place to ensure that system upgrades and configuration changes do not overwrite system patches	
	Is a process in place to track the application of and maintain a list of patches installed on all servers and standard workstation images?	
	Is a process in place to monitor the availability of system patches?	

	Is a process in place to track known vulnerabilities and to cross-reference this list with patch application information?	
6.2.8 **Remote and Local Management and Monitoring**	Is the local root or administrator password on servers changed every 30 days or immediately when a Security System Administrator leaves or is transferred?	
	Is the use of local or root UIDs and passwords strongly discouraged and instead are administrators required to have their own local server accounts with appropriate permissions for off-line access?	
	On Windows NT server systems is the administrator account renamed?	
	Is out-of-band management configured via modem and console port used to remotely connect to network devices for management purposes?	
	If out-of-band management is used, is the dial-in system left in an always-on state?	
	If out-of-band management is used, are the access numbers distributed only to system administrators?	
	What is the policy concerning how often edge device shell-exec passwords are changed?	
	Are system administration duties delegated such that no single system administrator is allowed system-wide privilege?	
	Are edge device configurations stored in a secure location on the network with limited user access?	
	Are edge device and other network equipment configurations not stored on portable equipment such as palm pilots and laptops that can be easily stolen?	

	Do edge devices support the use of TFTP to remotely configure them?	
	Are edge devices such as firewalls and routers configured to support remote management through the use of SNMP or Telnet?	
	Are separate read-only and read-write community strings that are appropriately cryptic set on all SNMP capable devices?	
	Is the capability to perform remote SNMP monitoring and sets restricted to only designated internal management workstations?	
	Are servers managed through the use of any of the following: terminal services, metaframe, telnet, or Web management agents?	
	Are router/hub/switch passwords changed regularly?	
	Are two levels of passwords, read-only and privileged assigned for router access?	
6.2.9 Logging and Alerting	Do edge gateway devices at a minimum log the following: Date, time, interface, action, service (port), source, dest, protocol (UDP, TCP, ICMP, ESP, etc), rule applied, source port, username, xlate source addr, xlate dest addr, xlate source port, xlate dest port?	
	Is there accountability tracking for all end-users capturing events that include: • Successful session log-ins? • log-in failures? • administration activities? • all actions by privileged users? • failed attempts to access information	

	Is there a mechanism in place to generate alerts based on the above audit events?	
	Does information for each record include: • user ID • information or system accessed • date and time of access • type of event • result of event • reason for failure (if applicable)	
	Are alarms enabled where the capability exists to indicate security breeches on all applicable platforms (Windows NT, AS400, Firewalls, Routers)?	
	Are there active network intrusion detection systems (NIDS) deployed on critical network segments such as the interconnection between the Internet and the corporation?	
	Are host or hybrid intrusion detection systems (HIDS) deployed on Internet accessible and mission critical servers?	
	Are logs from distributed systems gathered together in a secure central data storage area for inspection and reporting?	
	How often are firewall and access-list logs reviewed to confirm the validity of allowed and denied connections?	
	How often are Windows NT event, application, and security logs reviewed	
	Is there an incident response procedure and how often is it exercised?	

6.2.10 Configuration and Change Management	Does a configuration control methodology exist for all network-attached systems and are change requests validated as coming from authorized individuals?	
	Is a software tracking system being used for security change management?	
	Are security configuration changes, upgrades, and updates approved and documented by a security policy committee consisting of administrators and executive decision makers?	
	What formal or informal security design review procedure is applied to changes, upgrades, and updates and at what stage(s) of the process?	
	Do individuals responsible for altering systems or application software obtain authorization through approved change management procedures?	
	Do all modifications to existing computer systems undergo controlled testing prior to becoming a part of an operational system?	
	How do multiple system administrators pass system security configuration information between themselves and log changes?	
	Does documentation exists that provides descriptions of system hardware, software, network diagrams, and components and is this documentation stored online in a secure location?	
	Is a duplicate copy of each set of configuration documentation stored with backup procedures in a secure off-site location subject to date, timestamp and version number control procedures?	

	How many third party consultants have access to these information resources?	
6.2.11 **Personal Information Protection and Electronic Documents Act**	Please outline at a high level Hydro's concerns with respect to federal government policy outlined in Bill C-6. Are the bulk of Hydro's concerns related to employee privacy, customer privacy, international partner privacy or all of these?	
	Has Hydro's legal department specifically identified personal information that can and/or cannot be collected and stored in electronic format and the protection measures that must be put in place to safeguard this information?	
	Does Hydro clearly identify the purpose for the collection of personal information to be stored in electronic format?	
	Does Hydro always obtain the consent of its customer's to store this type of information and to use this information for business purposes?	
	Does Hydro limit the collection of personal information to the bare minimum of that which is required to do business?	
	Does Hydro limit the time period that personal information will be stored after a customer no longer subscribes to Hydro's services?	
	Does Hydro make every effort to limit the use of personal information to only that required to perform business with the end customer?	

	Does Hydro take specific measures to ensure the accuracy of information such as calling the customer back at their registered phone number to ensure that it is in fact the customer who is calling when changes to personal information are requested?	
	Does Hydro make their information and electronic data handling policies known to their customers?	

7 Internet Access

7.1 General

7.1.1 Internet access topology	Describe your Internet access topology.	
	How are firewalls used to restrict in-bound and out-bound traffic?	
	Describe how DNS servers are used.	
	Describe how SMTP servers are used.	
7.1.2 Internet Applications	What servers / applications require access to the Internet (e.g. Credit Card checking)?	
	Describe how security is implemented to protect these servers.	
	What servers / applications need to be accessed from the Internet (e.g. Hydro customer web page)?	
	Describe how security is implemented to protect these servers.	
7.1.3 Internet usage policies	What policies have been put in place to govern Internet usage with regards to restricting access to particular sites?	
	What policies have been put in place to govern Internet usage with regards to non work related usage ?	

7.1.4 Web Caching	Is Web Caching used? If so, where do the caching devices logically reside in your network?	
	Please describe the hardware used for web caching. If a server or workstation is used, please reference the device from the section 1.	
	Please describe the software used for web caching.	

Appendix D

Project Plans

HYDRO
THE POWER OF
COMMITMENT

Local Area Network (LAN)

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1.0 Project Summary

The purpose of this project is to create a reliable, scaleable and manageable LAN/WAN for Hydro utilizing Layer three switching, VLAN and Gigabit Ethernet technologies. Where possible redundant layer three switches and a router redundancy protocol will be utilized to provide redundant inter-VLAN routing. Layer three switching offloads inter-VLAN route processing from the WAN routers, promoting the use of VLANs. Additional VLANS at Hydro will:

- Improve network performance by decreasing the broadcast domain.
- Enhance security when access-lists are implemented between VLANS.

The new network will support aggregate Gigabit Ethernet technology to supply bandwidth scaleable to 16 gigabits.

- Four core switching designs are utilized through-out the Hydro network:
- Fully redundant chassis based layer three switch.
- Dual fixed configuration layer three switch.
- Dual layer two-switched core.
- Layer three switch with integrated T1 WAN interface.

Which of the four designs gets implemented in an area office is mainly dependent on the “class of office” representing user count and projected growth at the location. The various classes of office are defined as follows:

- **Hydro Place Data Centre** – This location is the core of Hydro’s computing environment hosting major corporate applications and providing connectivity to over half the company’s users.

- **Large Office** – These are large sites with greater than 75 users. The sites that fall into this category are Bishop’s Falls and Churchill Falls.

- **Medium Office** – These are medium size sites with between 26 and 74 users. The sites that fall into this category are Holyrood and Bay D’Espoir.

- **Small Offices** – These are small sites with 25 or less users that have connectivity to the corporate WAN. The sites that fall into this category are Whitbourne, Stephenville, Port Saunders, St. Anthony, Deer Lake, Wabush and Happy Valley.

- **Remote Offices** – These are company locations that do not have connectivity to the corporate WAN and must use remote access methods to utilize corporate applications. These sites include all remaining office, depot, substation, home access and mobile user locations.

Based on the above, Hydro Place will receive a chassis based layer three switch at the core with enough Gigabit connectivity to support Gigabit connections to the access layer. Each wiring closet will comprise its own VLAN at this location and an Executive VLAN used to facilitate security. Full redundancy will be achieved in year two by adding redundant supervisors, route processors and line cards to the core switch. Redundant route processors can utilize a router redundancy protocol and provide automatic fail-over capability for inter-VLAN routing. As well the additional Gigabit interfaces at the core will allow for aggregate connections to the access layer, increasing bandwidth and redundancy.

Churchill Falls and Bishops Falls, as “Large Office” locations, will utilize a dual fixed configuration layer three switch design at the core and Gigabit connections to the access layer. Location based VLANS will be created at these locations to decrease the broadcast domain and increase security. VLAN load balancing using the Spanning tree protocol will be utilized to increase bandwidth and redundancy for the access layer connections at these locations. The two layer three switches at these locations can utilize a router redundancy protocol and provide automatic fail-over capability for inter-VLAN routing.

The Holyrood and Bay D’ Espoir core, as “Medium Office” locations, will be comprised of dual layer two switches for redundancy, and a mixture of Gigabit and 100Mbps connections to the access layer. At these locations the same switches can be used at the access layer and the core. The use of VLANS will be limited at these locations to reduce the load on the router.

The remaining sites, as “Small Office” locations, including Whitbourne, Stephenville, Port Saunders, St. Anthony, Wabush, Happy Valley and Deer Lake are locations with 25 or fewer users and no anticipated growth. A Layer three switch with integrated T1 WAN interface will be installed at each of these locations.

2.0 Scope

This project is limited to network devices on the administration network only, excluding the SCADA and substation components.

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:

Benefits:

- Removal of the final vestiges of Token Ring architecture from Hydro's network. This will result in Hydro have an industry standard network infrastructure, with a lower cost per component requirement than the existing proprietary network.
- Increased performance, and elimination of source-route bridging requirements
- Increased manageability through enabling of SNMP management on all network devices
- Increased security through the creation of VLAN's

Risks:

- Forces the final migration of any remaining Token Ring devices, resulting in potential investment in legacy platforms

4.0 Deliverables

The following deliverables will be produced throughout the course of the project:

Deliverable	Description
Physical install L3 Switch	• Rack new switch and connect to existing 5506.
Location based VLANS	• Create VLANS and trunk connection to existing switch.
L3 switching between VLANS	• Remove the VLAN sub-interfaces from the 7206 and configure L3 routing on new switch.
Redundant, load balancing Gigabit backbone.	• Configure Gigabit connections between access layer devices and aggregate Gigabit connections between access layer and core switch.

5.0 Strategy / Approach

<u>Hydro Place</u>

Rack the Chassis based layer three switch in the communications room and connect to existing network via a 100Mbps Ethernet over fiber connection. This is a fiber connection because the 5506 is located in the computer room and the new switch is destined for the communications room. Install the access layer switches in computer room and create location based VLANS, servers VLAN and Executive VLAN. The servers VLAN should maintain the existing network otherwise clients and external servers will loose access to these devices. Enable a routing protocol on the new switch and ensure it gets and accurate routing table.

The Internet connection for the building terminates in the communications room and a 10Mbps Ethernet over fiber connection carries it to the external router in the computer room, another 10Mbps fiber connects the Inside interface on the PIX to the 7206 router in the communications room. The Internet connection, external router and PIX can now move to the communications room.

The inter-VLAN routing function can now move to the new layer three switch and its virtual interface should become the default gateway for all Ethernet clients on the Hydro Place LAN. Configure the router redundancy protocol to provide automatic fail-over for inter-VLAN routing. The servers VLAN clients are currently using the 7206 router as their gateway, the easiest way to make the default gateway change is to change the IP address on the 7206 and use its address on the new switch, this way no change is required on the servers. The DHCP server at Hydro Place must be configured with new scopes to supply IP addressing for the additional VLANS and the PIX modified to permit Internet access for the new IP networks.

Install access layer switches in the wiring closets and configure aggregate Gigabit connections to each closet. Upgrade all Token Ring based desktops with Ethernet connectivity. Each wiring closet will comprise a separate VLAN meaning each client connected to the new switches must get new IP addressing: a re-boot may be required. When all Token Ring clients are migrated to Ethernet the 5506 can be retired and the Token Ring interface on the 7206 disabled.

The network management station must be configured to monitor the new core switch and access layer devices. SNMP read and write community strings must be agreed upon and implemented on the devices.

Configure access-lists on the layer three switch to secure the VLANS.

Install and configure a proxy server. After all clients on the Hydro Place LAN are configured to use the Proxy server for Internet access modify the PIX configuration to allow only the proxy server. The use of a Proxy server and a NT global group called “Internet Users” provides the ability to enable or disable a users Internet access based on NT user account.

Create an internal primary and secondary DNS with authority for the “nlh.nf.ca” Domain and add “A” records as required for internal hosts. The DNS’s could be

NT 4.0 based or Windows 2000 based. A Windows 2000 based DNS will support DDNS (Dynamic DNS) and ease a future move to Windows 2000. If Windows 2000 based DNS's are used they cannot be Domain Controllers for the NLH NT Domain and should be configured a standalone servers. These DNS's will be configured as forwarders for Caching DNS' at the remote sites.

Churchill Falls

Rack the fixed configuration layer three switches in the communications room and the access layer switches in the third floor wiring closet of the C&A Building. Install access layer switches in the Warehouse, Powerhouse and Fire and Safety buildings and connect to the core. Configure redundant Gigabit connections to the access layer and create VLANS.

Configure the router redundancy protocol to provide automatic fail-over for inter-VLAN routing. Maintain the existing IP network number for the servers VLAN to avoid client access to server issues. The default gateway for the servers VLAN will be the WAN router and this should be changed to the layer three switch virtual interface. The best way to make this change is to move the IP address on the router to the layer three switch virtual interface and put a new address on the router. Configure additional DHCP scopes to support the new VLANS.

The network management station must be configured to monitor the new core switch and access layer devices. SNMP read and write community strings must be agreed upon and implemented on the devices.

Configure access-lists on the layer three switch to secure the VLANS.

Install and configure a proxy server on the NT file and print server. After all clients on the LAN are configured to use the Proxy server for Internet access modify the PIX configuration to allow only the proxy server. The use of a Proxy server and a NT global group called "Internet Users" provides the ability to enable or disable a users Internet access based on NT user account.

Create a caching DNS on the NT file and print server and configure it to forward unknown requests to the internal DNS's at Hydro Place. If the request cannot be serviced by these DNS's it will be forwarded on to the Internet based DNS's. The other two locations in Churchill Falls do not require redundancy but SNMP manageable layer two switches must be installed.

Holyrood

Rack layer two switches in the communications room, the third floor wiring closet (offices) and the Mechanical Workshop. Connect one of the core switches to the

Ethernet hub in the communications room. Configure redundant Gigabit connections from the core switches to the office wiring closet and redundant 100Mbps connections to the Mechanical Workshop. **xwave** recommends redundant fiber connections to the training center and the warehouse, 100mbps connections will suffice for these connections. Use of VLANS will be limited at this location because the inter-VLAN routing must be performed at the WAN router. Create VLANS to enhance security and administration.

The servers at this location are currently Token Ring attached. After all the desktops are migrated to Ethernet and the servers are the only devices using the old IP address network, the servers can be migrated and the Servers VLAN assigned the old IP address network. The token Ring interface on the router must be disabled at this time to avoid IP routing problems.

The network management station must be configured to monitor the new core switchs and access layer devices. SNMP read and write community strings must be agreed upon and implemented on the devices.

Install and configure a proxy server on the NT file and print server. After all clients on the LAN are configured to use the Proxy server for Internet access modify the PIX configuration to allow only the proxy server. The use of a Proxy server and a NT global group called “Internet Users” provides the ability to enable or disable a users Internet access based on NT user account.

Create a caching DNS on the NT file and print server and configure it to forward unknown requests to the internal DNS’s at Hydro Place. If the request cannot be serviced by these DNS’s it will be forwarded on to the Internet based DNS’s.

Bishops Falls

Rack the fixed configuration layer three switches in the communications room and access layer switches in the Security Building, Service Building and the Diesel Plant. Configure redundant Gigabit connections to the access layer and create VLANS.

Configure the router redundancy protocol to provide automatic fail-over for inter-VLAN routing. Maintain the existing IP network number for the servers VLAN to avoid client access to server issues. The default gateway for the servers VLAN will be the WAN router and this should be changed to the layer three switch virtual interface. The best way to make this change is to move the IP address on the router to the layer three switch virtual interface and put a new address on the router. Configure additional DHCP scopes to support the new VLANS.

The network management station must be configured to monitor the new core switch and access layer devices. SNMP read and write community strings must be agreed upon and implemented on the devices.

Configure access-lists on the layer three switch to secure the VLANS.

Install and configure a proxy server on the NT file and print server. After all clients on the LAN are configured to use the Proxy server for Internet access modify the PIX configuration to allow only the proxy server. The use of a Proxy server and a NT global group called “Internet Users” provides the ability to enable or disable a users Internet access based on NT user account.

Create a caching DNS on the NT file and print server and configure it to forward unknown requests to the internal DNS’s at Hydro Place. If the request cannot be serviced by these DNS’s it will be forwarded on to the Internet based DNS’s.

Bay D’ Espoir

Rack layer two switches in the communications room, and all outlying buildings. Alternate the fiber connections from the five outlying buildings between the core switches. To achieve redundancy install additional NIC cards in the server and router and connect to both of the core switches. At this point each core switch will have a spare GBIC slot which could be used to increase the backbone bandwidth, or provide redundant Gigabit connectivity to a server. Use of VLANS will be limited at this location because the inter-VLAN routing must be performed at the WAN router. Create VLANS to enhance security and administration.

The network management station must be configured to monitor the new core switchs and access layer devices. SNMP read and write community strings must be agreed upon and implemented on the devices.

Install and configure a proxy server on the NT file and print server. After all clients on the LAN are configured to use the Proxy server for Internet access modify the PIX configuration to allow only the proxy server. The use of a Proxy server and a NT global group called “Internet Users” provides the ability to enable or disable a users Internet access based on NT user account.

Create a caching DNS on the NT file and print server and configure it to forward unknown requests to the internal DNS’s at Hydro Place. If the request cannot be serviced by these DNS’s it will be forwarded on to the Internet based DNS’s.

Remaining locations

Rack the layer three switch with integrated T1 WAN interface and connect all desktops. Coordinate the re-provisioning of the existing leased service with the service provider before connecting it to the router.

6.0 Schedule Summary

Site	Date
Hydro Place	Year 1
Bishop's Falls	Year 1
Bay D'Espoir	Year 1
Holyrood	Year 1
Churchill Falls	Year 2
Deer Lake	Year 2
Port Saunders	Year 3
St. Anthony	Year 3
Stephenville	Year 4
Happy Valley - Goose Bay	Year 4
Wabush	Year 5
Whitbourne	Year 5

7.0 Assumptions

Horizontal wiring in all locations is certified category 5e or better and vertical wiring is fiber based certified at 1 Gigabits.

HYDRO
THE POWER OF
COMMITMENT

Wide Area Network (WAN)

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1.0 Project Summary

The purpose of this project is to create a reliable, scaleable and manageable, IP protocol based WAN for Newfoundland and Labrador Hydro (Hydro).

When complete, the end user will see improved network performance by reducing latency through the increase of usable bandwidth by the integration of internet & and mission critical applications on common facilities. The deployment of T1 cards in routers and increased access speeds will reduce serialization delays.

The project will also provide improved network reliability by implementing ring-based architecture to support major sites where Hydro's private infrastructure & Frame Relay services exist.

Routers will be upgraded where necessary to support traffic peaks during failed conditions, QoS features and the latest interactive applications. For the most part this will include the addition of T1 cards in the 2600 & 3600 series routers and the replacement of routers in the following sites:

- Whitbourne,
- Stephenville,
- Port Saunders,
- St. Anthony,
- Wabush,
- Happy Valley
- Deer Lake

These locations have 25 or fewer users and no anticipated growth. A Layer three switch with integrated T1 WAN interface will be installed.

2.0 Scope

This project is limited to network devices on the administration network only excluding the SCADA and substation components.

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:
Benefits:

- Improved network performance by reducing latency through the increase of usable bandwidth by the integration of internet & and mission critical applications on common facilities.
- The deployment of T1 cards in routers and increased access speeds will reduce serialization delays.
- Improved network reliability by implementing ring-based architecture to support major sites where Hydro's private infrastructure & Frame Relay services exist.
- Support traffic peaks during failed conditions, QoS features and the latest interactive applications.

Risks:

- Merging different network elements onto a one WAN design increases the opportunity for the failure of a single element to create outages in multiple services.
- Increased cost as the development of a ring architecture requires leasing facilities from a carrier.
- Accelerates the requirement to develop QoS expertise within Hydro's technical employee base.

4.0 Deliverables

The following deliverables will be produced throughout the course of the project:

Deliverable	Description
Service Intergration	• Replace Leased point to point bandwidth with Frame Relay.
Router upgrades	• Deploy T1 cards in 3600's &2600's
7206 upgrade	• Add 8 port T1 card to 7206
Create redundant IP WAN Ring	• Upgrade services to complete at Deer Lake, Central, St. John's ring
Router Replacements	• Replace low end routers with integrated router/switch

5.0 Strategy / Approach

<u>All Sites</u>

Increase Frame Relay access speed at all location to support both mission critical and internet / intranet-based applications. The immediate requirements will consist of the summation of the frame and leased services port rates.

In conjunction with feedback from network management system statistics, implement QoS routing features to support queuing techniques to allocate priorities to the mission critical traffic.

Hydro Place

Deploy 8-port T1 card in the 7206 and upgrade network processor engine to support the same. The T1 card will be the IP gateway for NF Hydro's private radio network. Integrate all remote Frame Relay traffic on the OC3 using FRATM PVC's to each remote site. Employ traffic shaping on the 7206 OC3 egress port to ensure that congestion takes place within the router and not in the carrier network.

Churchill Falls

Increase frame bandwidth to 1.536Mbit/s and terminate on existing FT1 card.

Holyrood

Install a T1 card in 2600 and establish a dedicated T1 to the 7206 over the private radio facility. Out order the frame & leased services that are not required.

Stoney Brook

Provision 100M facility to Ethernet port on existing 3600 and provision 2 Mbit/s PVC to OC3 at Hydro Place. Provision T1s to Deer Lake, Bishop Falls and Bay D'Espoir and connect to new T1 cards installed in the Stoney Brook router.

Bishops Falls

Establish a T1 to Stoney Brook and deploy T1 card in router.

Bay D' Espoir

Establish a T1 to Stoney Brook and deploy T1 card in router.

Remaining locations

Rack the layer three switch with integrated T1 WAN interface card. Coordinate the re-provisioning of the existing frame services with the service provider before connecting it to the router.

Location A	Location Z	BW Kbits/s
Port Saunders	St. John's	128
Springdale	St. John's	128
St. Anthony	St. John's	256
Stephenville Office	St. John's	128
Wabush Office	St. John's	128
Whitbourne	St. John's	256

6.0 Schedule Summary

Phase	Date
Holyrood T1 Card	Year 1
Bishop’s Falls T1 Card	Year 1
Bay D’Espoir T1 Card	Year 1
Stoney Brook T1 Card	Year 1
Add T1 Card to 7206 HP	Year 1
CFLCo T1 Card	Year 2
Deer Lake 4224	Year 2
Port Saunders 4224	Year 3
St. Anthony 4224	Year 3
Happy Valley 4224	Year 4
Stephenville 4224	Year 4
Springdale 4224	Year 5
Wabush 4224	Year 5
Whitbourne 4224	Year 5

7.0 Assumptions

Assumes existing routers have maintenance contracts for IOS upgrades if required.

HYDRO
THE POWER OF
COMMITMENT

Internet

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1.0 Project Summary

The purpose of this project is to create a secure, scaleable and manageable, broadband Internet portal at Hydro Place.

When complete the end user will see improved network performance through the use of full-duplex 10M access and reduced latency of a typical Internet query.

The project will also provide improved network security, as the topology will utilize a dedicated facility thus eliminating risks associated with the shared accesses (e.g. network discovery and multicast-storms).

2.0 Scope

Implement a broadband Internet solution. Broadband refers to Internet accesses of 10 Megabits per second and above.

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:

Benefits:

- Creates a secure, scaleable and manageable, broadband Internet portal at Hydro Place
- Improved network performance through the use of full-duplex 10M access and reduced latency of a typical Internet query.
- Improved network security through use of a dedicated facility, eliminating risks associated with the shared accesses

Risks:

- Nil.

4.0 Deliverables

The following deliverables will be produced throughout the course of the project:

Deliverable	Description
Establish New Internet Access	• Replace existing half-duplex internet portal with full-duplex portal
Router Replacements	• Replace existing low end 2500 gateway router with 1751 10Mbit/s full duplex router
Negotiate SLA with ISP	• Document measurable performance parameters and negotiate terms for the exceeding and failing to meet the terms

5.0 Strategy / Approach

Hydro Place

Negotiate terms of service with an ISP to deliver full-duplex dedicated Internet portal, which will provide greater price/performance than the existing service. Document measurable performance parameters and negotiate terms for the exceeding and failing to meet the terms. Replace the existing low-end 2500 gateway router with 1751 10/100Mbit/s full-duplex router. Configure the new router to minimize the risk of network discovery and attack.

6.0 Schedule Summary

Milestone	Date
Full-duplex dedicated Internet Portal	Year 1

HYDRO
THE POWER OF
COMMITMENT

Servers

Project Plan
December 2001

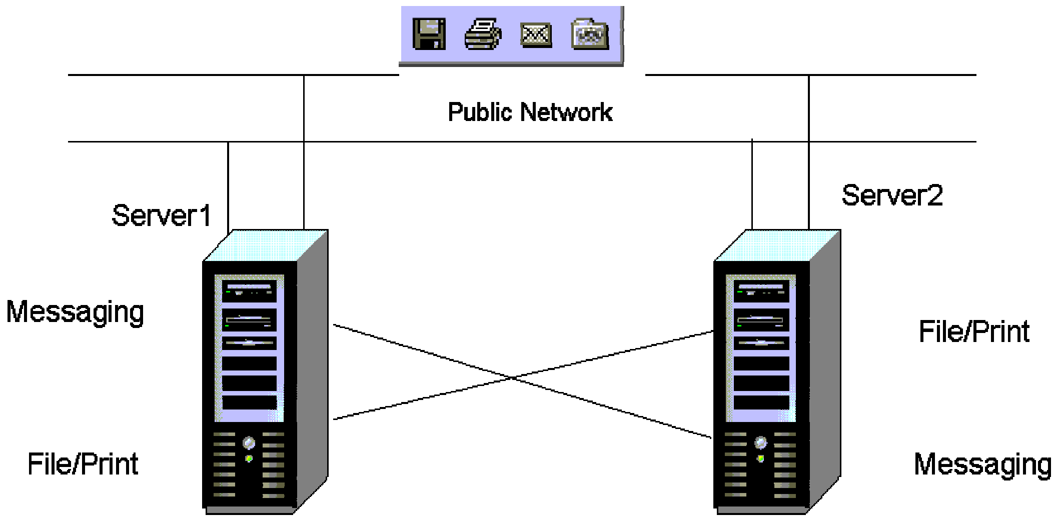
xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

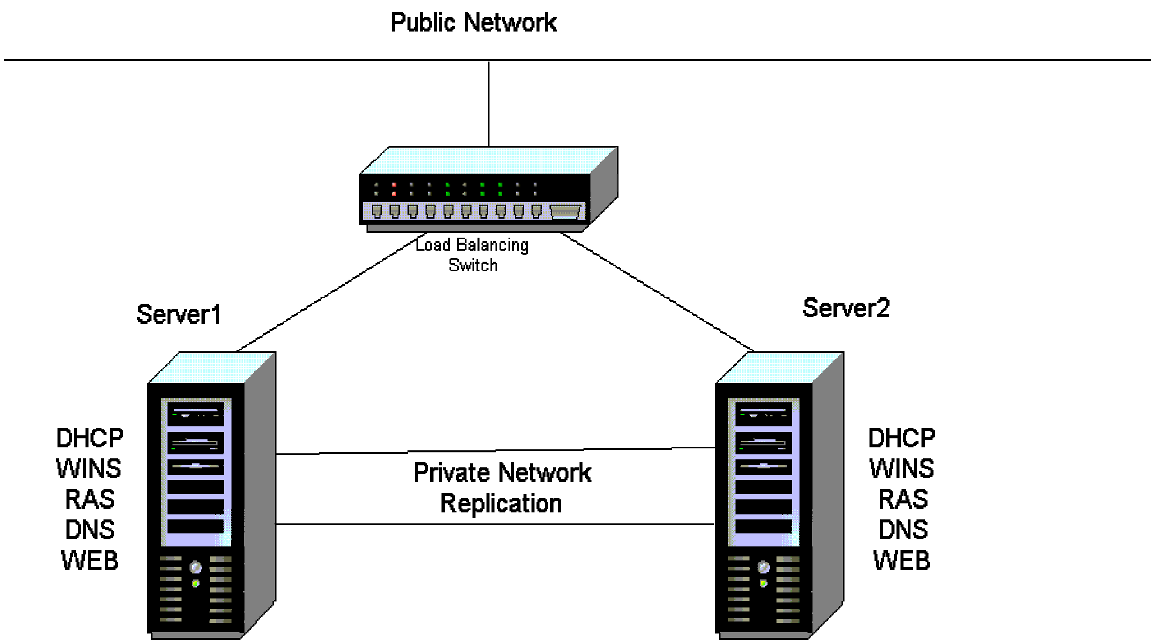
Table of Contents

1.0 Project Summary

The server infrastructure at Newfoundland Hydro is responsible for hosting and maintaining service to the end-user client base, and consists of both core application and network servers housed at Hydro Place, and file/print and messaging servers distributed throughout the WAN. Given the requirement for 99.99% availability for these services it is necessary to full redundancy and High Availability (HA) clustering configurations for all servers. As with other elements of the network, there must not be any single point of failure in the design. The type and level of HA and redundancy varies depending on the type of server infrastructure in question. For distributed file/print and messaging servers the long-term technical design includes the implementation of a small cluster environment in the location, with one functional server providing an HA cluster to the other. That is, the file/print server would back up the messaging server, and vice versa.



For core network services the long-term technical design recommends creation of functional clusters. That is, servers that provide primary network functionality, such as DNS/WINS, Authentication, etc., would be provisioned in a functional cluster with a load-balancing switch in front.



Under this scenario there would be mirror images of the functional servers that would provide backup for each other in the event of a failure. Automatic failover would be achieved through the load-balancing switch configuration (also redundant) in that, if one server became unavailable, the entire load would switch to the available server.

The purpose of this project is to create a reliable, scaleable and manageable server infrastructure for the Remote Office File/Print and Messaging as well as Functional servers.

The results of the project include:

- An increase in the availability of services through the deployment of Microsoft Clustering.
- Hardware upgrades applied to existing servers.
- A replacement of older servers with new models.

A plan has been developed for each remote site. The actual steps involved in each plan depend upon the server infrastructure currently at each site.

Servers at each site will be set up as follows:

1. One server will run Lotus Domino Services.
2. One server will run File/Print Services, Functional Services (Secondary WINS, Backup Domain Controller, Web Caching, Proxy

Services), Installation Services for Local Installed applications and Network applications, and Local applications.

Some sites have specific applications that will also be set up within the Cluster.

2.0 Scope

This project is limited to the following types of servers:

- Remote File/Print and Messaging,
- Functional Services.

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:

Benefits:

- Increased availability / redundancy in all server infrastructure deployed both within Hydro Place and in the field.
- Support for mission-critical applications through achieving 99.99% availability
- Upgrading of server infrastructure to a standardized model and image, resulting in lower TCO.

Risks:

- Creates an immediate requirement for expertise in clustering technologies, which have proven problematic in the past.
- Deploys high-end technology in remote locations, which may result in increased remote management difficulty.

4.0 Deliverables

The following deliverables will be produced throughout the course of the project.

Deliverable	Description
Server Clusters in various sites	• Install / upgrade servers with Microsoft Clustering and Shared Storage arrays.

5.0 Strategy / Approach

Hydro Place

Set up a test lab at Hydro Place.

1. Identify the Cluster Storage requirements. Establishing the Cluster requirements will determine the best approach to take when setting up the Clusters at the remote sites.
2. Identify the hardware and software requirements for servers in a cluster.
3. Set up test servers.
4. Install and configure a test Cluster Storage Unit.
5. Create the first node (server) in the test cluster and configure the second node (server) to join the cluster.
6. Configure file and print services in the cluster.
7. Install and configure applications for failover. This test should include the services and applications that will be found in the remote sites.
8. Install, configure, and test proxy and caching Services in the cluster.
9. Test various failover scenarios of the cluster.
10. Document findings.

It is important to note that some steps for each site can be performed prior to visiting the site. This will cut down on the time required at each site.

Holyrood

Review and confirm the server environments for HOB3, HOM1, HOM2, and HOM3. Initial indications are that HOB3 and HOM2 will be the servers in the cluster. Identify any additional hardware and software requirements that are not present in the servers. HOB3 will require Microsoft Windows 2000 Advanced Server as the operating system. The HOM2, which was purchased in 1998, will be replaced. A cluster storage unit will also be required.

Create parts list and order any additional components.

Install and configure the new HOM2 server for Windows 2000 Advanced Server. Upgrade HOB3 to Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (HOB3) of the cluster. Configure HOM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino and Eta-Pro to HOM2.

Install proxy and web caching services on HOB3.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Bishops Falls

Review and confirm the server environments for BFB1, BFM2, and BFM3. Initial indications are that BFB1 and BFM2 will be the servers in the cluster. Identify any additional hardware and software requirements that are not present in the servers. BFB1 will require an additional 768MB of memory as well as Microsoft Windows 2000 Advanced Server as the operating system. BFM2 will require 256MB of memory, an additional 733MHz CPU, and Windows 2000 Advanced Server. A cluster storage unit will also be required.

Create parts list and order any additional components.

Upgrade BFB1 and BFM2 with the additional components and Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (BFB1) of the cluster. Configure BFM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino to BFM2.

Install proxy and web caching services on BFB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Bay D’ Espoir

Review and confirm the server environments for BDB1 and BDM2. Identify any additional hardware and software requirements that are not present in the servers. BDB1 will require an additional 256MB of memory as well as Microsoft Windows 2000 Advanced Server as the operating system. The BDM2 server, which was purchased in 1998, will be replaced. A cluster storage unit will also be required.

Create parts list and order any additional components.

Install and configure the new BDM2 server for Windows 2000 Advanced Server. Upgrade BDB1 with the additional components and Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (BDB1) of the cluster. Configure BDM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino to BDM2.

Install proxy and web caching services on BDB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Churchill Falls

Review and confirm the server environments for CFB1, CFB2, CFB3, CFM4, CFM5, and CFM6. Initial indications are that CFB1 and CFM5 will be the servers in the cluster. Identify any additional hardware and software requirements that are not present in the servers. CFB1 will require 512MB of memory, an additional 733MHz CPU, and Windows 2000 Advanced Server. CFM5 will require an additional 256MB of memory as well as Microsoft Windows 2000 Advanced Server as the operating system. A cluster storage unit will also be required.

Create parts list and order any additional components.

Upgrade CFB1 and CFM5 with the additional components and Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (CFB1) of the cluster. Configure CFM5 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino from CFM3 and CFM6 to CFB1.

Install proxy and web caching services on CFB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Port Saunders

Review and confirm the server environment for POB1. Identify any additional hardware and software requirements that are not present in the server. A new server, POM2, will be purchased. A cluster storage unit will also be required.

Create parts list and order any additional components.

Install and configure POB1 and the new POM2 server for Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (POB1) of the cluster. Configure POM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino to POM2.

Install proxy and web caching services on POB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

St. Anthony

Review and confirm the server environment for SAB1. Identify any additional hardware and software requirements that are not present in the server. A new server, SAM2, will be purchased. A cluster storage unit will also be required.

Create parts list and order any additional components.

Install and configure SAB1 and the new SAM2 server for Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (SAB1) of the cluster. Configure SAM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino to SAM2.

Install proxy and web caching services on SAB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Happy Valley - Goose Bay

Review and confirm the server environment for HVB1. The HVB1, which was purchased in 2000, will be replaced. A new server, HVM2, will be purchased. A cluster storage unit will also be required.

Create parts list and order any additional components.

Install and configure HVB1 and the new HVM2 server for Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (HVB1) of the cluster. Configure HVM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino to HVM2.

Install proxy and web caching services on HVB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Stephenville

Review and confirm the server environment for SVB1. The SVB1, which was purchased in 2000, will be replaced. A new server, SVM2, will be purchased. A cluster storage unit will also be required.

Create parts list and order any additional components.

Install and configure SVB1 and the new SVM2 server for Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (SVB1) of the cluster. Configure SVM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino to SVM2.

Install proxy and web caching services on SVB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Appendix A contains the list of services on the servers in Stephenville before and after the implementation of the cluster.

Wabush
Review and confirm the server environment for WAB1. The WAB1, which was purchased in 2000, will be replaced. A new server, WAM2, will be purchased. A cluster storage unit will also be required.

Create parts list and order any additional components.

Install and configure WAB1 and the new WAM2 server for Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (WAB1) of the cluster. Configure WAM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino to WAM2.

Install proxy and web caching services on WAB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Appendix A contains the list of services on the servers in Wabush before and after the implementation of the cluster.

Whitbourne

Review and confirm the server environment for WBB1. The WBB1, which was purchased in 2000, will be replaced. A new server, WBM2, will be purchased. A cluster storage unit will also be required.

Create parts list and order any additional components.

Install and configure WBB1 and the new WBM2 server for Windows 2000 Advanced Server.

Install and configure the cluster storage unit. Create the first node (WBB1) of the cluster. Configure WBM2 to join the cluster. Configure file/print services in the cluster. Install and configure the local applications and services that will reside on the servers in the cluster. Migrate Lotus Domino to WBM2.

Install proxy and web caching services on WBB1.

Test the failover capabilities of the cluster by shutting down one server in the cluster. After a successful test, repeat the test for the other server in the cluster.

Additional PC Servers

A number of smaller PC servers exist in Hydro. While these servers probably do not have a requirement for clustering, some of these servers were purchased in 1996 and 1997. These systems should be replaced. The table below shows the PCs that should be replaced and the type of workstation server recommended as replacement.

Server	Current Function	Configuration	Estimated Cost

DNS1	Standalone Server 1. Microsoft External DNS for NLH.NF.CA 2. Microsoft IIS Web Server for WWW.NLH.NF.CA	IBM IntelliStation M Pro Pentium 4 1.4GHz CPU 256 MB Memory 30 GB disc Microsoft Windows 2000	$2,740
TRV-1_DC	Standalone Server 1. SQL Database Server 2. Plant Ledger	IBM IntelliStation M Pro Pentium 4 1.4GHz CPU 256 MB Memory 30 GB disc Microsoft Windows 2000	$2,740
TR4-2_D2	Standalone Server 1. MIMS	IBM IntelliStation M Pro Pentium 4 1.4GHz CPU 256 MB Memory 30 GB disc Microsoft Windows 2000	$2,740
TR3-3_DC	Standalone Server 2. Human Resources Database Server	IBM IntelliStation M Pro Pentium 4 1.4GHz CPU 256 MB Memory 30 GB disc Microsoft Windows 2000	$2,740

It is important to note that TRV-1_DC, TR4-2_D2, and TR3-3_DC run OS2 Warp as their operating system software. The applications on the PC servers may have to be ported to Windows 2000.

6.0 Schedule Summary

Milestone	Date
1. Create test cluster	Year 2
2. Establish cluster at Holyrood	Year 2
3. Establish cluster at Bishop Falls	Year 2
4. Establish cluster at Bay D'Espoir	Year 2
5. Establish cluster at Churchill Falls	Year 2
6. Establish cluster at Port Saunders	Year 3
7. Establish cluster at St. Anthony	Year 3
8. Establish cluster at Happy Valley	Year 4
9. Establish cluster at Stephenville	Year 4
10. Establish cluster at Wabush	Year 5
11. Establish cluster at Whitbourne	Year 5

7.0 Assumptions

- Windows 2000 Advanced Server is noted as the Operating System for the Server Clusters. As newer OSs are introduced by Microsoft, the Operating System may change. For example, in Years 3,4,and 5 the OS may not be Windows 2000 but rather a follow on product.
- New servers are named with reference to the site. Naming standard requirements may result in names of new servers changing.
- Server specifications and costing are for budgeting purposes. Servers with similar capabilities from other vendors may also meet the requirements.

8.0 Critical Success Factors

The following factors are critical to the success of the project:

- This project is dependent upon the timelines for the Windows 2000 Migration Project. A delay in that project may delay this project’s timelines

HYDRO
THE POWER OF
COMMITMENT

End User Infrastructure

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1.0 Project Summary

One component of the Hydro IT Technical Architecture Strategy project is the long-term technical design for end-user infrastructure. Specifically, it is the way in which the end-users in the organization interact with both each other and the enterprise. As indicated in the Vision, employees will primarily use electronic methods to communicate within the enterprise, and with this in mind the long-term technical design has significant implications on the way people will complete their job functions in the future. In developing the long-term technical design for the end-users consideration must be made of the future functionality to be delivered. Specifically, the differences in people's location and job function dictate different approaches to implementing end-user infrastructure. The Business Needs Research identified a variety of ways in which employees use the existing IT infrastructure. One classification is:

> **Support Staff** – Support staff provide staff functions such as HR, Finance, Engineering, etc. that are used by the production functions to manage and complete their tasks. Some support staff are located in each regional office to perform duties such as time entry, inventory management, etc. Most support staff utilize a variety of office productivity tools as well as accessing core applications, such as JD Edwards or the future Document Management service. In addition, some support staff in specialized roles require access to specialty applications such as load flow design software for engineering departments, etc. In general, support staff perform most of their job function in their primary office location.

For support staff much of the interaction with core applications will be dictated by the architecture for each application. Core applications will utilize a four-tier architecture whereby the end-user will interact with the system using a thin client arrangement. The specific thin-client architecture will be dictated by the location and function of the support staff. For those in support positions that do not require much local processing or specialized applications, the thin client architecture of choice is the use of an appliance device. Under this scenario a support person in a remote office would use an appliance with a smart card to work on JD Edwards, perform time entry, request reports or documents from the Data Warehouse, etc. For those support positions where a significant amount of end-user processing is required, such as conducting financial analysis, or where specialized applications are required, such as Computer Aided Design or Geographic Information Systems, a thin client arrangement using an application such as Citrix would be used. This would provide the end-user with a combination of local desktop processing power, as well as thin client access to the core applications. As with the server infrastructure, the desktop / laptop configurations would be based on standardized configurations.

The purpose of this project is to create a reliable and efficient thin client infrastructure implementing a combination of thin client appliances and Citrix Metaframe for Support Staff.

2.0 Scope

This project is limited to the following types of staff:

- Support Staff located in remote offices.

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:

Benefits:

- Reducing the Total Cost of Ownership for distributed computing resources through standardization on a lower cost, thin-client model. This results in easier troubleshooting, centralized software upgrades and simplified sparing.
- Increasing security by creating a standardized configuration in the field that cannot be manipulated by the end-user.
- Increased mobility for the work force as any thin client device on the network will be able to provide the same tools as the user's primary location.

Risks:

- Increased demands on LAN/WAN infrastructure as clients must access information over the network, instead of locally.
- Potential user backlash at the loss of desktop computing power.

4.0 Deliverables

The following deliverables will be produced throughout the course of the project:

Deliverable	Description
Deliver Thin Client technology to support staff in sites outside of Hydro Place	• Install Citrix Metaframe servers in remote sites • Migrate users from desktops to thin client appliances.

5.0 Strategy / Approach

Planning Phase

Prior to any migration, a planning exercise must be completed. During this exercise, the following steps are performed:

1. Identify Sites for migration
2. Identify applications in use at each site
3. Review Network communications environment
4. Estimate file storage requirements
5. Identify Metaframe server requirements
6. Review existing Domain for integration of Metaframe servers
7. Application Installation testing and documentation
8. Backup Client configuration and testing including restore of Active Directory objects
9. Citrix / Microsoft License Management testing and documentation
10. Client Printing Methods testing and documentation
11. Assemble Documentation
12. Get PO and Approval

The following table contains an example of the required configurations for a Metaframe Server and a thin client appliance.

Hardware Function	Component
Citrix Metaframe	IBM x330 with dual PIII 1260MHz CPUs 768 MB Memory 2 64GB discs
	Microsoft Windows 2000 OS software
	Microsoft Windows 2000 Client Access Licenses
	Microsoft Windows Terminal Services Client Access Licenses
	Citrix Metaframe XPe Client Access Licenses
Thin Client Appliance	Wyse WinTerm 1200LE

Once the planning exercise has been completed, a pilot migration can take place. The purpose of the pilot is to test the functionality and acceptance of the thin client technology.

Hydro Place

Set up a pilot at Hydro Place:

1. Receive server hardware and software
2. Install and configure Metaframe server
3. Install Standard desktop software and local applications on Metaframe server
4. Configure Thin Client appliances to point to Metaframe server
5. Test Thin client connectivity to Metaframe server
6. Test desktop software / applications / lotus Notes
7. Migrate users to thin clients / remove desktops

After the pilot migration has been in place for a length of time (1 – 3 months), determination must be made as to whether thin client technology meets the requirements of the support staff and reduces the requirements for desktop support.

If it is determined that there are cost savings and user acceptance with the thin client infrastructure, then migrations in the remote sites should commence.

It is important to note that some steps for each site can be performed prior to visiting the site. This will cut down on the time required at each site.

The proposed Thin Client solution is focused on remote sites only. However, should an implementation at Hydro Place be considered, pricing is provided for a 40-user rollout.

The following steps would be performed for each site that is being migrated to a thin client infrastructure.

<u>Remote Sites</u>

1. Review planning exercise for validity in current site.
2. Receive server hardware and software.
3. Install and configure Metaframe server.
    a. Install and configure Server Hardware (CPU, RAM, Drives, etc)
    b. Install hardware into racks (including wiring)
    c. Configure Drives, install Windows 2000 Server and MetaFrame XP
    d. Configure and test communications
    e. Configure and test Backup software
4. Install Standard desktop software and local applications on Metaframe server
    a. Install Standard image software
    b. Install site specific applications

   c. Connect server to File / Print server directories

5. Configure Thin Client appliances to point to Metaframe server
6. Test Thin client connectivity to Metaframe server
7. Test desktop software / applications / lotus Notes
8. Migrate users to thin clients / remove desktops
   a. Backup desktop data and port to file server
   b. Install Thin client on desktop
   c. Remove old desktop

6.0 Schedule Summary

Milestone	Date
1. Create pilot thin client infrastructure	Year 2
2. Establish thin client infrastructure at Holyrood	Year 2
3. Establish thin client infrastructure at Bishop Falls	Year 2
4. Establish thin client infrastructure at Bay D'Espoir	Year 2
5. Establish thin client infrastructure at Churchill Falls	Year 2
6. Establish thin client infrastructure at Port Saunders	Year 3
7. Establish thin client infrastructure at St. Anthony	Year 3
8. Establish thin client infrastructure at Happy Valley	Year 4
9. Establish thin client infrastructure at Stephenville	Year 4
10. Establish thin client infrastructure at Deer Lake	Year 4
11. Establish thin client infrastructure at Wabush	Year 5
12. Establish thin client infrastructure at Whitbourne	Year 5

7.0 Assumptions

- The current evergreen process of replacing desktops can be categorized by site. This results in preventing desktops in a site that is about to be configured for thin client from receiving new desktops that would have to be replaced shortly.
- Staff at Hydro Place are not included in this project at this time.
- Each site will require its own Metaframe server. In the event of a failure in the WAN, a Metaframe server in each site assures users will be able to access local file/print servers and local email services.
- Server specifications and costing are for budgeting purposes. Servers with similar capabilities from other vendors may also meet the requirements.

8.0 Critical Success Factors

- This project is dependent upon the timelines for the Windows 2000 Migration Project since Citrix Metaframe XP is based upon Windows 2000. A delay in that project may delay this project’s timelines.

HYDRO
THE POWER OF
COMMITMENT

Security

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1.0 Project Summary

This security project is being created to address a number of short term recommendations that should be addressed to enhance the Hydro's overall security. This project must work in conjunction with all other enhancements in place for the Hydro computer network and technologies. The prime areas of security that this project will address include:

- Create an effective Security Policy document
- Plan for the implementation of a single sign-on solution
- Address remote vendor support issues
- Plan for Hydro to conduct routine vulnerability assessments
- Centralized log monitoring and analysis
- Implement Intrusion Detection Systems in key locations

2.0 Scope

Security Policy: The development of security policies will include the review of the current policies, organizing workshops to establish security policy objectives, researching risk involved in new IT technologies and presenting the security policy to senior management for approval.

Single Sign-on: A single sign-on solution will involve many steps over the next 3-5 years. The initial step includes expansion of the securId authentication to key computer applications. Further steps to achieve the goal of single sign-on include establishing a strategy to minimize the mixture of technologies used to supply computer applications and review of new developments in the single sign-on technology.

Remote Vendor Support: This issue will first need to be addressed within the corporate security polices, after the corporate objective related to remote vendor support is determined and implementation policy will be completed.

Routine Vulnerability Assessments: This project will require the acquisition of tools to assess security, a corporate policy that supports routine testing of all computer systems and trained personnel able to perform these tests on a scheduled and ad hoc basis.

Centralized log monitoring and analysis: This project will establish a centralized database to receive log data from all key computer systems. Using advanced log analysis tools, this information will be analyzed to determine the state of security for Hydro's computer infrastructure.

Intrusion Detection Systems: This project will identify key locations to place network based and system based Intrusion Detection Systems (IDS). The project will also include the centralized administration of this service and the required process to effectively respond to security alerts.

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:

Benefits:

- Creates a structure for developing Hydro's overall security policy. The structure or framework can then be populated by the various elements, such as IDS, single sign-on, etc., in a coordinated manner.
- Leverages the activities undertaken in other project plans to maximize the value for Hydro's security.

Risks:

- Security can be viewed as an intangible benefit without a defined payback period, and as a result is often more difficult to justify to external stakeholders.
- Implementation of technology and policy must be done in conjunction with development of ownership by the staff at Hydro, or else the effort will have reduced effectiveness.

4.0 Deliverables

The following deliverables will be produced throughout the course of the project:

Deliverable	Description
Comprehensive Security Policy documentation	• Security policy document that clearly identifies Hydro's strategy to manage security risks.
Develop a Single sign-on Solution multiple phased plan	• A multiple phase plan to move Hydro's network to a complete single sign-on solution over the next 3-5 years.
Establish a policy for remote vendor support	• A key facet of the security policy development will include a comprehensive policy regarding remote vendor support.
Implement tools to support the remote vendor access policy	• The required tools will be identified and implemented to effectively provide vendors with remote

	access while maintaining the integrity of the corporate policy standards.
Vulnerability assessments requirements and procedures	• Identify and acquire the electronic tools required, identify training requirements and the processes required to routinely test Hydro's computer network and systems for vulnerabilities.
Project plan to establish a centralized log management and reporting	• Identify the centralized data base tools required, establish communication links and procedures to spool critical log information to centralized data repository and develop reports for analysis of this information into comprehensive management reports.
Plan for implementation of Intrusion Detection Systems	• Identify the areas within the Hydro computer network to strategically locate IDS systems. These systems will include network based IDS as well as IDS systems running on key application servers.

5.0 Strategy / Approach

Security Policy:

A security policy is the key foundation to a comprehensive security program. The security policies will address; management ownership, a risk management review process, process to approve exceptions to the policy, technical standards for all technologies and a process to update the policy as technology and business environments change. The approach to develop security policies will include:

- Review of all existing policies
- Conduct workshops to determine the appropriate security "balance" and security "strategy"
    - Workshops will include both management and technical staff from all departments within Hydro
- Creation of a draft security policy document
- Review the draft security policies with Hydro to make the necessary "fine tuning" adjustments

- Complete a final security policy document
- Present policy standards to upper management for security policy formal approval
- Prepare implementation plan to communicate security policy standards to employees

Single Sign-on:

The implementation of single sign-on will not be a quick process. Time and patience will be required to implement the different phases with the ultimate objective of a true single sign-on solution. This project will develop a multiple phased plan to work towards a single sign-on solution.

> Phase 1: This phase will be implemented within a relatively short period of time and should be completed in year 1. This phase will involve the establishment of a centralized authentication process to simplify the authentication for Hydro's users.
>
> - Expand the SecurID authentication process to all key systems
>   - Evaluate and implement SecurID authentication client on a number of existing systems
> - Expand the distribution of SecurID token cards to all employees who require computer access
> - Establish a plan for minimizing the computer technologies in use at Hydro.
>
> Phase 2: Over the next 1-3 years the successful development of SSO technology should be reviewed and evaluated for use within Hydro. The maturation of this technology is expected to provide effective solutions with this time period to enable Hydro to meet their ultimate goal of a complete Single Sign-On solution.
>
> Phase 3: Includes the final implementation of Single Sign-On. The effort, costs and issues involved cannot be accurately determined at this time.

Remote Vendor Support:

The corporate strategy and policy regarding remote vendor support will be addressed during the development of security policies with Hydro. Upon full understanding of the requirements an implementation plan and review procedure will be established to review all current access to ensure that it meets the security standards. This plan will include:

- Review remote access technologies in place at Hydro to determine whether they meet the policy standards.
- Select the appropriate technology to provide remote access vendor support.
- Review all current remote access in use by vendors.
- Convert the existing vendors to the appropriate remote access method
- Establish a procedure for review of all new requests for remote access for vendors.

Routine Vulnerability Assessments:

Conducting an initial vulnerability assessment will allow Hydro to test the effectiveness of the security controls implemented on their different computer systems. Conducting this assessment on a routine basis will ensure that the security standards are maintained over time and will raise a warning if the results of a future test vary from the original baseline. This project will include the following activities:

- Review vulnerability assessment tools
- Select appropriate tools for use
- Perform initial vulnerability test on all systems
- Identify any security adjustments that should be made on existing systems
- Document vulnerability assessment procedure and schedule.

Centralized log monitoring and analysis:

Although xwave recommends that Hydro centralize and automate logging as much as possible it is not possible given the wide variety of applications and technologies in use to completely centralize logging facilities. Distributed logging mechanisms to gather data are often quite practical while distributed reporting and presentation systems are usually not. xwave recommends that Hydro centralize reporting and presentation of log data gathered from distributed operating systems, firewalls, routers, and IDS agents as much as possible. Since no one product currently exists on the market that addresses reporting for the complete suite of Hydro hardware and software, it will be necessary to develop a custom front-end HTML reporting server and SQL server that will query the distributed log databases for presentation information. This project will include the following activities:

- Review logging procedures and capabilities on all systems
    - Logging will be essential from all Firewalls, IDS systems, and authentication systems
    - Review the logging capabilities for all operating systems and applications

- Activate the appropriate level of logging on the systems
- Establish a centralized database for logs
- Establish processes to transmit logs to the database
- Develop a custom HTML reporting system
- Document procedures to generate and review regular management reports.

Intrusion Detection System:

This project will identify key locations to place network based and system based Intrusion Detection Systems (IDS). The project will also include the centralized administration of this service and the required process to effectively respond to security alerts.

- Evaluate the strategic locations for implementation of IDS solutions.
    - Include both network and server based IDS
- Determine the appropriate IDS solutions for Hydro
- Implement complete IDS systems with central management and monitoring
- Create procedures for monitoring and managing alerts.
- Create a security incident response escalation plan

6.0 Schedule Summary

Milestone	Date
Security Policy	Year 1
Single Sign-On	
Phase I: Centralized Authentication	Year 1
Phase II: Research and Evaluation	Year 3
Phase III: Final Implementation	Year 4
Remote Vendor Support	Year 1
Routine Vulnerability Assessments	Year 1
Centralized Log Monitoring and Analysis	Year 2
Intrusion detection System	Year 2

7.0 Assumptions

The following assumptions have been made related to the project:

Security Policy:

- Active participation in the workshops will be required from many key individuals within Hydro.
- Hydro will assign one or more individuals as prime to review the draft policies and assist in the “fine tuning” exercises.

Single Sign-on:

- That single sign-on technology will continue to be enhanced to include most applications and operating systems currently in use at Hydro.
- The commitment to a long term single sign on solution will be a business objective over the next 3-5 years.

Remote Vendor Support:

- The security policies will include Hydro’s strategy in relation to providing remote access for vendors
- This project assumes that some remote vendor access will be authorized by the security policy
- The security policy project will be completed before this project commences.

Routine Vulnerability Assessments:

- An ongoing commitment will be made to invest in the time required to conduct regular vulnerability assessments
- The individuals responsible to conduct the vulnerability assessments are properly trained to interpret the test results.

Centralized log monitoring and analysis:

- Current logging technology does not exist to manage the logs of all systems in use at Hydro
- An ongoing commitment will be made to review the security reports and respond appropriately

Intrusion Detection System:

- Hydro will make the commitment to monitor IDS alerts and follow a reasonable escalation procedure.
- The IDS program will be frequently reevaluated and adjusted as business needs dictate.

8.0 Scope Limitations

The following are limitations to the project:

Security Policy:

- The security policies will include general security standards for the different operating systems, but will not include full system design standards for these systems.

Single Sign-on:

- Phase 1 of the project will establish centralized authentication using SecurID
- A plan will be developed to review single sign-on technology for phase 2 and 3 of this project
- The cost estimates for phase 2 and 3 are based on too many variables to allow calculation at this point in time.

Remote Vendor Support:

- This project will not take into consideration any investments or changes that vendors will be required to implement in order to remotely connect to Hydro's computer network.

Routine Vulnerability Assessments:

- This project does not include training Hydro staff regarding security vulnerabilities identified by the vulnerability tools and the measures required to mitigate these risks.

Centralized log monitoring and analysis:

- The effort required to develop the HTML reporting system are based on assumptions of the basic reports that Hydro will require.

Intrusion Detection System:

- As the computer network and systems within Hydro grow and change over time, the IDS design must be adjusted to effectively monitor activity.

9.0 Critical Success Factors

The following factors are critical to the success of the project:

Security Policy:

- Participation from key representatives from all departments within Hydro are key to the success of developing an effective security policy
- Security policies require support from upper management to be successful
- A security awareness program would be required to communicate the security policy information to Hydro employees.

Single Sign-on:

- The number of technologies that Hydro will connect to a single sign-on solution is minimized.

- The complexity of the single sign-on environment will have a direct impact of the cost and difficulty of this project.

Remote Vendor Support:
- Management support to control the remote access for vendors will be required to ensure the success of this project.

Routine Vulnerability Assessments:
- Proper training in the use of the vulnerability testing tools and understanding of the security vulnerabilities will be a key factor to the success of this project.
- The vulnerability testing tools will require regular upgrades to be able to identify new vulnerabilities.

Centralized log monitoring and analysis:
- All key systems will extract their log information to the central database
- Intrusion Detection Systems will be strategically located throughout the Hydro computer network
- A rigorous process will be followed to regularly review log reports

Intrusion Detection System:
- A dedication to monitor and react to security alerts is essential for IDS to be effective.
- An effective security escalation procedure is required to react properly to security situations

HYDRO
THE POWER OF
COMMITMENT

Network Management

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1.0 Project Summary

The reliance by Newfoundland Hydro staff on the services provided by their corporate IT (administrative) systems and infrastructure has increased over the years to the point that these services have now become mission critical in supporting the primary business of (and operational systems for) power generation and distribution.

While the reliance on corporate IT systems and infrastructure has increased, the capability to manage and sustain these has not increased proportionally, particularly in light of the increasing complexity of these systems.

The purpose of this project is to design and implement a Network Operations Center (NOC) to enable enterprise level management of Newfoundland Hydro's corporate IT systems throughout Newfoundland according to industry standard IT Service Management model "best practices". The guiding principle of IT Service Management is that IT services are there solely to support the business and its efficient and effective operation. The three main objectives of Service Management are:

- To align IT services with current and future needs of the business and its customers;
- To improve the quality of IT services delivered; and
- To reduce the long term cost of service provision.

The NOC will be the physical nerve center for the equipment and personnel whose primary function is to keep the Newfoundland Hydro corporate systems infrastructure running smoothly. It will be comprised of a team of network, operational and customer support specialists who monitor the IT infrastructure and provide troubleshooting and customer support (i.e. Help Desk) services 24 hours a day, 365 days a year.

2.0 Scope

This project plan outlines the steps necessary for the implementation of a NOC within Newfoundland Hydro for the management of the corporate IT (administration) systems and infrastructure only. Although there are numerous IT components within the operational systems (i.e. Energy Management System), the management of those systems and infrastructure is outside the scope of this project.

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:

Benefits:

- Centralized monitoring and control of network elements, reducing the TCO for deployed infrastructure.
- Consolidation of network monitoring capabilities to create economies of scale.
- Conversion from a reactive method of network management to a proactive method, which can reduce both the frequency and duration of outages.

Risks:

- Successful implementation of a Network Management system is dependant both on technology and development of appropriate processes. If the processes are not structured properly Hydro will not reap the full benefit of its investment.
- Much of the Network Management project is dependant on successful implementation of the other projects in the program.

4.0 Deliverables

The following deliverables will be produced in the course of the project.

Deliverable	Description
Preliminary Project Plan	• High level, long-term plan providing strategy/approach to the project, budgetary cost estimates, and desired major milestones & dates
Project Charter	• Documents what the project is to achieve and how the results will be realized
Detailed Project Work Plan	• Detailed plan providing refined budget, schedule and level of effort estimates based upon the Requirements Specification • ‘Baseline’ plan which is modified throughout remainder of project to reflect chosen design (e.g. training components)
Requirements Specification	• Documents functional and non-functional requirements determined from analysis of current and desired managed elements/environments; usage, process and data integrations; and business processes

Preliminary Design Specification	• Documents overall solution architecture, tools, integrations and required organizational and process flows
Detailed Design Specification	• Detailed documentation of management infrastructure setup; element instrumentations; integrations; deployments (e.g. prototypes, rollouts); and process flows
Acceptance Test Plan	• Detailed documentation of tests to be conducted to prove that the acceptance criteria specified for all of the functional and non-functional requirements documented in the Requirements Specification have been met. • Includes methods, sequencing, timings and expected results for all tests

5.0 Strategy / Approach

The implementation of a Network Operations Center is a daunting task for any organization at any time due to its complexity and impact on all areas of the business. Due to the likelihood of multiple IT upgrade/enhancement projects taking place concurrently with the NOC Project, placing severe demands on the IT staff and user population at Newfoundland Hydro, xwave recommends a careful, phased approach in the scheduling of this project. In developing the estimated high level project schedule, we were careful to take into account the recommended project schedules in the other IT project plans, as well as to minimize the number of concurrent tasks during the project. This will help minimize the time demands on Newfoundland Hydro's employees and the stresses involved in adjusting to multiple concurrent changes in their work processes and environment.

The recommended overall strategy is the use of xwave's standard "plan, design, build, operate" methodology, with some modifications necessary for this type of project.

The planning phase should involve detailed requirements analysis. In addition to the traditional focus on technical functional requirements, the Process Team will need to conduct a detailed analysis of current and desired business processes as they pertain to the management of the IT infrastructure at Newfoundland Hydro. Also during this phase, a detailed Project Plan should be written as a baseline and maintained and updated throughout the remainder of the project as requirements, design and circumstances dictate.

The design phase should ensure that the technical and business requirements identified during the planning phase are mutually supportive and technically feasible. A preliminary (high level) design specification identifying the recommended solution set or sets for meeting the documented requirements should be produced, reviewed and approved prior to proceeding with a detailed design and specification.

The build phase should involve the careful development, testing and implementation of each of the tools and technologies identified in the design specification. Acknowledgement and approval that the solution has met the requirements is obtained by formally conducting the tests documented in the Acceptance Test Plan and having the appropriate project authority sign-off each test.

The operate phase should involve the transfer of responsibility from the project team to the group responsible for ongoing operation of the NOC. If it has not already taken place, adequate overlap time must be allocated to ensure effective “transfer of technology” has taken place between the project and operations teams. On this point, xwave strongly recommends that the staffing for long-term operations of the NOC be determined as early in the project as possible, and that the operations staff assist with and/or observe as much as is practical during the “build” phase. Our experience has shown that this is a period when high levels of learning are achieved, and with the added benefit of being a period of low ‘consequence of error’ to the business.

6.0 Schedule Summary

The table below indicates the estimated major milestone timelines for implementation of the various capabilities provided in or by the NOC. The dates specified assume a project commencement date of January 1, 2002, and do not take into account critical path analysis which would be determined during the detailed Project Work Plan. In addition, time estimates are based upon a median level of Service Management implementation. The time estimates would also be revised one the Requirements Specification is completed and the level of desired implementation, staffing levels etc. is fully known.

Milestone	Date
Project Commencement	01 JAN 2002
Project Charter Delivered	14 JAN 2002
First Draft of Detailed Project Work Plan Delivered	04 FEB 2002
Requirements Analysis Complete	01 APR 2002
Requirements Specification Delivered	15 APR 2002
Preliminary Design Specification Delivered	13 MAY 2002
Detailed Design Specification Delivered	29 JUL 2002

Milestone	Date
Physical NOC Center completed	09 SEP 2002
Acceptance Test Plan Delivered	23 SEP 2002
Remote Monitoring (up/down status) for all monitored network nodes in production	21 OCT 2002
Incident Management (Service Desk) in production	21 OCT 2002
Service Continuity (Disaster Recovery) Plan completed	31 DEC 2002
Remote Application/Server Monitoring for all monitored systems in production	03 MAR 2003
Problem Management in production	21 APR 2003
Desktop Management integration in production	16 JUN 2003
Configuration Management in production	28 JUL 2003
Change Management in production	22 SEP 2003
Performance Monitoring of required services in production	29 DEC 2003
Automated Service status web reporting in production	26 JAN 2004
Storage Area Network Management integration in production	26 JAN 2004
Security Management Integration in production	23 FEB 2004
Capacity Management in production	19 APR 2004
Service Level Management Integration in production	18 OCT 2004
Availability Management in production	13 DEC 2004
Service Level Reporting Integration in production	10 JAN 2005

7.0 Assumptions

The following assumptions have been made related to the project:

- Newfoundland Hydro Senior Management will be committed to the success of this project
- Necessary resources will be made available and will be dedicated to the project
- An appropriate physical site for the NOC is available with industry standard High Availability HVAC, UPS and security systems in Hydro Place, requiring only the installation of network management servers and consoles.

8.0 Scope Limitations

The following are limitations to the project:

- In order to minimize any delays and/or rework, the NOC plan will need to developed and monitored to effectively mesh with the implementation phases of the other infrastructure upgrade projects running in parallel with this project. Careful coordination and effective communications between the various Project Managers and teams will be needed to accomplish this.

- Before design can effectively be completed, significant process changes need to be identified, agreed upon, and documented which will provide the guidelines and direction of the Design Phase.

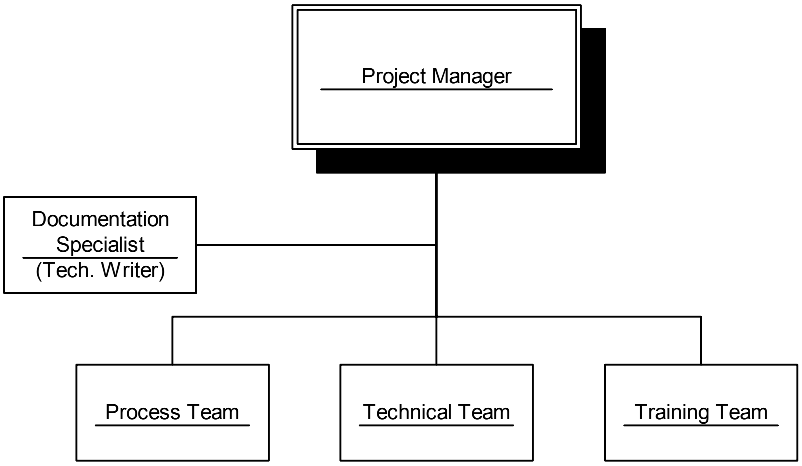
9.0 Critical Success Factors

The following factors are critical to the success of the project:

- Availability and commitment of appropriate Newfoundland Hydro resources.
- Access to personnel, documentation, and information needed by the Project Team.
- Decisions made in a timely manner at key milestones to ensure project continuity.
- Timely response to requests for information, particularly defining process and functional requirements.
- Commitment of and sponsorship by the senior management of Newfoundland Hydro is essential, particularly in light of the impact on people and processes that this project will entail (i.e. changes). Senior management sponsorship will ensure that the project is seen as the company's new way of doing things as opposed to "something else IT is shoving at us".
- High Level Project governance through a Project Sponsor and Steering Committee.
- "User Buy-In" is essential for this project to succeed. The best way to achieve this is to establish an effective communications plan for disseminating information to the user community. In addition, user input/feedback should be encouraged during all phases of the project where feasible, but particularly during the requirements analysis phase.
- By far the most important factor for the success of this project is for the project team and senior management to keep the focus on meeting business objectives and processes, and not on the technology being implemented. This will ensure that the appropriate tools are selected during the design phase, and that the correct level of integration and management is implemented to meet the needs of the business (i.e. correct project scope is maintained).

10.0 Project Organization

The recommended composition of the Project Team dedicated to the NOC project is as follows:



The complexity of the NOC project indicates that a full-time senior Project Manager is essential for planning, coordinating and tracking all activities throughout the duration of the project.

A Documentation Specialist, ideally a technical writer, is required to assist with the development of the large number of documents to be created during the course of the project. In particular, there is likely to be a significant amount of documentation required for the business, service support and service delivery processes.

The Process Team's focus will be on analyzing and documenting the current business processes as they relate to IT management within Newfoundland Hydro, and then assisting Newfoundland Hydro staff in determining and documenting what the IT service management processes should be. The Process Team should consist of staffs who are seasoned business analysts, preferably with experience and/or training in IT Service Management "best practice" processes such as those documented in the IT Infrastructure Library. At a minimum, the Process Team should consist of one senior and one intermediate business analyst.

The Technical Team's focus will be on analyzing the technical requirements for the network operations center within Newfoundland Hydro, developing a design, and implementing and testing it. This will involve a careful mapping of the tools of service management in such a way as to best meet the business requirements and processes of Newfoundland Hydro. The Technical Team should consist of staff with varying degrees of experience and/or training in IT management products. At a minimum, the Technical Team should consist of one senior, one intermediate, and one junior IT management specialist. In addition, technical experts in various technologies in place at Newfoundland Hydro will be required a various times throughout the project to assist with the implementation and configuration of monitoring and management tools.

The Training Team's focus will be on determining the training needs for all employees of Newfoundland Hydro, from the NOC operators and administrators to the Service Desk representatives and end users of the corporate systems. At a minimum, the Training Team should consist of an experienced Training Coordinator who can liaise between employees and 3rd party trainers if training is outsourced.

HYDRO
THE POWER OF
COMMITMENT

Storage Area Network (SAN)

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1.0 Project Summary

The purpose of this project is to provide a fiber channel based SAN (Storage Area Network) for Newfoundland and Labrador Hydro (Hydro. This project is a three phase project a data backup & recovery component, a data storage component, and a branch/remote office component. The first two phases are to be implemented within the data center at hydro place. The data backup & recovery phase focuses moving these services to a switched fiber channel fabric and deploying multiple small-mid sized tape libraries. The data storage phase will build upon the existing infrastructure deployed in the previous phase. This phase involves adding redundancy to the fiber fabric and server interconnects, installing central storage enclosures and disk, and moving application data into the SAN. The final phase focuses on deploying SAN technologies in the regional and remote offices. The key criteria in determining whether or not SAN technologies will be deployed in a specific regional/remote office are the existence of cluster technologies.

2.0 Scope

The following key points identify the activities that sit within the scope of the SAN Project:

- This project is focused solely on data stored on disk or tape.
- This project will deploy a fiber channel based infrastructure for the storage, backup, & recovery of production data.
- This project will deploy management software required to monitor and manage the physical and logical elements of the SAN

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:

Benefits:

- Consolidation of storage activities through development of a SAN results in increased data integrity, backup capabilities and efficiency in network resource use.
- Provides a complete solution for data management at Hydro Place.
- Builds on Hydro’s existing expertise in data management through its experience with Veritas and TSM.

Risks:

- SAN technology is still evolving, and as a result timing of infrastructure investment is key to avoiding stranded investment

4.0 Deliverables

Deliverable
Tape backup/recovery
Centralized data storage
Storage infrastructure for Clusters in regional offices
SAN Management infrastructure

5.0 Strategy / Approach

In order to ensure the appropriate solution is successfully deployed xwave will perform a storage assessment for each phase of the project. The storage assessment will focus on the specific components being deployed during each phase. Once the storage assessment is complete the specific hardware will be ordered and installed.

6.0 Schedule Summary

Milestone	Date
Phase I: Data Backup / Restore	Year 1
Phase II: Data Storage	Year 2
Phase III: Branch and Remote	Year 3

7.0 Scope Limitations

The following are limitations to the project:

- There is limited Fiber channel support for mainframe and AS/400 environments and the technologies that are available offer limited functionality or are prohibitively expensive. It is for these reasons that these environments may have to be addressed in a separate project.
- The focus of this project is on production data, any none production data or systems will not necessarily be addressed by this project or may be addressed as a secondary additional option.
- The project does not include the deployment of a Backup/Recovery software solution, that is being addressed under a different project.

8.0 Critical Success Factors

The following factors are critical to the success of the project:

- Management support
- Resource availability
- Access to required systems is made available.

HYDRO
THE POWER OF
COMMITMENT

Windows Evolution

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1. Project Summary

Hydro is currently utilizing a single NT Domain on a Windows NT 4.0 Server platform for application and file and print services and Windows NT 4.0 Workstation for a desktop operating system. The goal of this project is to migrate the servers and NT Domain to Windows 2000 Server and Active Directory, and the desktops to Windows 2000 Advanced. xwave recommends upgrading the servers before the desktops so that Hydro can utilize the desktop deployment features of Windows 2000 and Active Directory. This strategy was used at NB Power during their migration to Windows 2000.

An in-place upgrade of the PDC at Hydro Place to Windows 2000 server will start the migration process and populate the Active Directory with the existing user and computer accounts. This server will maintain backwards compatibility until all the BDC's through-out Hydro are migrated to Windows 2000 Domain Controllers. The desktop migration at each location can be facilitated using Windows 2000 "Remote Installation Server's" and the "User State Migration Tool". Any Windows 2000 server can be a Remote Installation server and provide a central repository for desktop images. The User State Migration tool is used to identify and backup user specific data such as profile information and data files i.e. spreadsheets and word documents, and exclude everything else. This utility must be customized to suite Hydro's application base to ensure all data files are captured. This tool is being used successfully at NB Power.

2. Scope

The project includes the migration of existing servers and NT Domain to Windows 2000 Server and Active Directory, and desktops to Windows 2000 Advanced.

3. Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:

Benefits:

- Implementation of the Windows 2000 in the early 2003 timeframe, as recommended in this project, will provide for increased stability in the OS, resulting in fewer patch requirements and more maturity of the overall network design
- Moving to Windows 2000 will allow Hydro to avail of the many features associated with Active Directory, including network-aware appliances.
- The existing network OS, Windows NT4, will become increasingly difficult and expensive to support in a distributed environment. At some point, Microsoft will abandon its support for the older OS in favour of the Windows 2000 model.

Risks:

- Any major upgrade of core network OS requires significant planning, cost and downtime, with no guarantee of success. This is by far the greatest risk associated with moving to Windows 2000.
- By waiting until early 2003 to implement Windows 2000 in the core of the network, Hydro will be delaying benefit from some of the network efficiencies created by the new LAN design
- The longer Hydro delays in moving to Windows 2000, there will be a greater "leap forward" in technology required to reach the new implementation.

4. Strategy/Approach

Hydro Place

Initiate a planning session to discuss Active Directory site and Domain design, Dynamic DNS, Domain Controller placement and Remote Installation Server placement. Create a test environment by restoring a Hydro PDC and BDC to test servers. Use the test environment to document the upgrade procedure and test existing applications on Windows 2000. Use the test network to develop and deploy standard Windows 2000 desktop images. Up-front customization of the Windows 2000 Remote Installation Server and User State Migration tools will save time during the desktop roll-out.

Backup the PDC and start the Windows 2000 server in-place migration procedure. When this process completes ensure the NT 4.0 PDC service is running and test that the new server is visible in the Windows NT 4.0 Domain. xwave recommends that no other migrations be performed for a week or so to ensure there are no issues with the hybrid environment. NB Power encountered an un-known problem with their WINS environment at this point which was fixed by re-booting all the BDC's. The new Active Directory now has all the user and computer accounts from the Hydro NT Domain.

Migrate the BDC's at this location using one of the following methods:

- the in-place migration is used when the server hardware is not changing. It is the quickest method but it is difficult to recover from a failed migration.
- installing Windows 2000 on new hardware takes a little longer because of the restore time but is the safest because the old hardware is maintained. Move resources such as shares, printers and applications to the new 2000 Domain controller via tape. Using tape to transfer data is quicker and the same server name can be maintained on the old and new server providing a transparent upgrade from the client PC perspective.

Desktop upgrades are the most time consuming part of the migration process as detailed below:

- backup the complete desktop to the server or some other device, this could be gigabytes of data and take hours.
- execute the User State Migration tool which captures user specific information from the local disk, on average 100Megs of data and takes 10-15 minutes.
- download desktop image containing corporate applications and other customization from the Remote Install Server (RIS). This takes about 20 minutes.
- execute the User State Migration a second time to restore the user specific information to the local disk which may take another 20 minutes.

NB Power's policy is to keep the complete user backup on tape for a month in case the User State Migration tool misses data. The times mentioned in the preceding section were gathered during a conversation with a member of NB Power's desktop deployment team.

Churchill Falls

Backup the BDC at this location and migrate to Windows 2000 server using one of the following methods:

- The in-place migration is used when the server hardware is not changing. It is the quickest method but it is difficult to recover from a failed migration.

- Installing Windows 2000 on new hardware takes a little longer because of the restore time but is the safest because the old hardware is maintained. Move resources such as shares, printers and applications to the new 2000 Domain controller via tape. Using tape to transfer data is quicker and the same server name can be maintained on the old and new server providing a transparent upgrade from the client PC perspective.

Install the Remote Install Server (RIS) services and configure to offer the corporate desktop image created during the testing phase.

Desktop upgrades are the most time consuming part of the migration process as detailed below:

- Backup the complete desktop to the server or some other device.
- Execute the User State Migration tool which captures user specific information from the local disk.
- Download desktop image containing corporate applications and other customization from the Remote Install Server (RIS).
- Execute the User State Migration a second time to restore the user specific information to the local disk.

Holyrood

Backup the BDC at this location and migrate to Windows 2000 server using one of the following methods:

- The in-place migration is used when the server hardware is not changing. It is the quickest method but it is difficult to recover from a failed migration.
- Installing Windows 2000 on new hardware takes a little longer because of the restore time but is the safest because the old hardware is maintained. Move resources such as shares, printers and applications to the new 2000 Domain controller via tape. Using tape to transfer data is quicker and the same server name can be maintained on the old and new server providing a transparent upgrade from the client PC perspective.

Install the Remote Install Server (RIS) services and configure to offer the corporate desktop image created during the testing phase.

Desktop upgrades are the most time consuming part of the migration process as detailed below:

- Backup the complete desktop to the server or some other device.
- Execute the User State Migration tool which captures user specific information from the local disk.
- Download desktop image containing corporate applications and other customization from the Remote Install Server (RIS).
- Execute the User State Migration a second time to restore the user specific information to the local disk.

Bishops Falls

Backup the BDC at this location and migrate to Windows 2000 server using one of the following methods:

- The in-place migration is used when the server hardware is not changing. It is the quickest method but it is difficult to recover from a failed migration.

- Installing Windows 2000 on new hardware takes a little longer because of the restore time but is the safest because the old hardware is maintained. Move resources such as shares, printers and applications to the new 2000 Domain controller via tape. Using tape to transfer data is quicker and the same server name can be maintained on the old and new server providing a transparent upgrade from the client PC perspective.

Install the Remote Install Server (RIS) services and configure to offer the corporate desktop image created during the testing phase.

Desktop upgrades are the most time consuming part of the migration process as detailed below:

- Backup the complete desktop to the server or some other device.
- Execute the User State Migration tool which captures user specific information from the local disk.
- Download desktop image containing corporate applications and other customization from the Remote Install Server (RIS).
- Execute the User State Migration a second time to restore the user specific information to the local disk.

<u>Bay D’ Espoir</u>

Backup the BDC at this location and migrate to Windows 2000 server using one of the following methods:

- The in-place migration is used when the server hardware is not changing. It is the quickest method but it is difficult to recover from a failed migration.
- Installing Windows 2000 on new hardware takes a little longer because of the restore time but is the safest because the old hardware is maintained. Move resources such as shares, printers and applications to the new 2000 Domain controller via tape. Using tape to transfer data is quicker and the same server name can be maintained on the old and new server providing a transparent upgrade from the client PC perspective.

Install the Remote Install Server (RIS) services and configure to offer the corporate desktop image created during the testing phase.

Desktop upgrades are the most time consuming part of the migration process as detailed below:

- *Backup the complete desktop to the server or some other device.*
- *Execute the User State Migration tool which captures user specific information from the local disk.*
- *Download desktop image containing corporate applications and other customization from the Remote Install Server (RIS).*
- *Execute the User State Migration a second time to restore the user specific information to the local disk.*

<u>Remaining site with Windows NT 4.0 Domain Controllers</u>

Backup the BDC at this location and migrate to Windows 2000 server using one of the following methods:

- The in-place migration is used when the server hardware is not changing. It is the quickest method but it is difficult to recover from a failed migration.

- Installing Windows 2000 on new hardware takes a little longer because of the restore time but is the safest because the old hardware is maintained. Move resources such as shares, printers and applications to the new 2000 Domain controller via tape. Using tape to transfer data is quicker and the same server name can be maintained on the old and new server providing a transparent upgrade from the client PC perspective.

Install the Remote Install Server (RIS) services and configure to offer the corporate desktop image created during the testing phase.

Desktop upgrades are the most time consuming part of the migration process as detailed below:

- Backup the complete desktop to the server or some other device.
- Execute the User State Migration tool which captures user specific information from the local disk.
- Download desktop image containing corporate applications and other customization from the Remote Install Server (RIS).
- Execute the User State Migration a second time to restore the user specific information to the local disk.

Post Migration

After all BDC's across the Hydro WAN are migrated to Windows 2000 remove the NT 4.0 PDC service from the first server at Hydro Place. The 2000 Domain Controllers can now be switched to Native mode to take full advantage of Active Directory features such as Universal and nested groups.

5. Schedule Summary

Complete all Servers in Year 1 and Desktops in Year 2.

6. Assumptions

The following assumptions have been made related to the project:

- Hydro will continue to use Microsoft Operating System offerings.

HYDRO
THE POWER OF
COMMITMENT

Physical Facilities

Project Plan
December 2001

xwave
AN ALIANT COMPANY

NEWTEL
an Aliant company

Table of Contents

1.0 Project Summary

Physical facilities are required to accommodate various types of networking, communications and server equipment along with suitable levels of power, UPS and air conditioning. Partial completion of this project has been achieved by Hydro through its study to establish standardized IS&T rooms and data closets at all Hydro locations. A section of the resulting Hydro Design Brief titled Business Solutions & Support - Design Brief   - LAN Upgrade – Hydro Place, Bishop’s Falls & Holyrood Plant written by Carl Holm is included below. The brief identified four classes of IS&T rooms and a core room and outlined the requirements for Hydro Place, Bishops Falls and Holyrood. To complement this deliverable, other Hydro locations were evaluated and classified based on recent site visits to determine requirements to bring them up to standard.

Excerpt from “Business Solutions & Support - Design Brief   - LAN Upgrade – Hydro Place, Bishop’s Falls & Holyrood Plant

Core Rooms

These core rooms are used when a site services more than 250 User Devices. With this capacity, there should be a separation of communication equipment and server equipment. Core rooms must be powered directly from batteries or off of an on-line UPS. Where possible core rooms should also have access to backup fuel generated power. Furthermore, equipment should be protected by a non-water based, fire extinguishing system. Finally, the environment should be maintained between 15-25˚ C and 50% - 65% Humidity.

Core Telecommunication Room.

This room will manage the communication entrance facility, the core router(s), core switches, and core communication equipment. All core communications should pass through the core communications room before being distributed to other parts of a facility. This includes entrance facility cables.

Core Server Room.

This room will manage all essential servers and where possible, even non-essential servers.

IS&T Rooms

Class 1 IS&T Room: Combination of Distribution Switches and Servers

A Class 1 IS&T Room will have a minimum of three racks: server rack, switching rack, and a miscellaneous rack. A server rack will house all servers and their supportive components such as keyboard and monitor. The switching rack will contain patch panels, horizontal and vertical cable management, routers, switches and modems. The miscellaneous rack will house UPS and any miscellaneous equipment not defined on the other two racks.
The miscellaneous rack shall have two standard UPS systems. Both systems are designed to last 60 minutes under full load. The first system will be used for the servers. This system will be rated for a load of 2000 VA and shall be equipped with multi-port communications. Each server will have a separate communications port directly to the UPS. The second UPS system will be rated for 850VA and will be used for the switching rack. This second UPS shall support SNMP management and will be managed by the Network Centre.
Both switching racks and miscellaneous rack will have vertical cable management attached. In addition, horizontal cable management will be used as necessary.

Class 2 IS&T Room: Distribution Closets

A Class 2 IS&T Room is defined as a room designated to handle only horizontal network distribution. Therefore no servers are installed in such rooms. To handle switches, the UPS will be designed to handle a load of 500 VA for 60 minutes. UPS shall also support SNMP management. These rooms are to be securely locked and their access managed by IS&T.

A Class 2 IS&T Room will typically only have one required 19” open rack with vertical management and horizontal management as required.
If air-conditioning is required, a second rack will be used.

Class 3 IS&T Room: Satellite locations

A Class 3 IS&T Room, is designed for small building applications where a designated IS&T Room is not available and equipment is limited to a single router, switch and possibly one server. If a secure dedicated room is available then a single open rack maybe used. However, if a secure dedicated room is not available then the Class 3 IS&T Room will refer to a secure fully enclose 19" rack cabinet. This cabinet will house, all required LAN hardware including router, switch, server, UPS, and Air Conditioning Unit. The UPS will be designed to handle a load of 850 VA for 60 minutes and shall support either a multi-port communications or a SNMP depending on the site requirements.

Class 4 IS&T Room: LAN Extensions

A Class 4 IS&T Room recognizes that because of the distances between the IS&T Room and the user, not all users can be reached under the standard premise cabling requirements. Furthermore, premises such as warehouses and generating plants do not have any means of facilitating an intermediate IS&T Room Therefore, a Class 4 TR can be used. This is a secure fully enclosed cabinet that can be attached to the wall. It will have capacity to house a termination block, a switch and optional UPS. The optional UPS will be designed for a load of 200 VA for 60 minutes. The UPS shall support SNMP management.
Uninterruptible Power Supplies (UPS).

UPS

All UPS devices will be Powerware 9000 series On-line devices. These are currently being used throughout the corporation and by standardizing on these, Hydro will require fewer number of spares and support consistent management tools. The on-line design will ensure that the load is always powered off the inverter and only requires utility power, via a bypass switch, if the battery fails. The UPS will protect telecommunication equipment from the following power problems:

UPS shall have the following features:
19" Rack mountable
Support multi-port communications to servers. Used in class 1 and 3 IS&T Room
Support SNMP monitoring in class 1 and 4
Batteries are valve regulated and can be replaced without interruption of service.

Air conditioning

Liebert air conditioning units shall be used as a standard unit. Air conditioning units will be used only if there is evidence that temperatures can exceed 30˚C. Due to the nature of the units, each room should be evaluated on an individual basis.

Fire System

Fire extinguishing systems are outside of the scope of this project, however it is recognized that fire extinguishing agents for core rooms should not be water based.

This project builds on this base document to identify the requirements for each Hydro location and defines the equipment needed to conform to the standards detailed above.

2.0 Scope

Implement consistent physical facilities to support the IS&T infrastructure, including LAN/WAN networking, communications, server equipment and support infrastructure, at the following Hydro locations:

- Hydro Place
- Churchill Falls
- Bishop's Falls
- Holyrood
- Port Saunders
- St. Anthony
- Whitbourne
- Bay D'Espoir
- Deer Lake
- Stephenville
- Wabush
- Goose Bay

3.0 Benefits / Risks

While not an exhaustive list, some of the major benefits and risks associated with this project include:
Benefits:

- Increased security for the IS&T infrastructure. This is especially true in outlying areas where, previously, there has not been the same level of emphasis on integrity of the infrastructure.
- Increased reliability through reducing the change of accidental disruption of equipment causing outages

- Increased control over environmental factors that may cause or exacerbate failure conditions

Risks

- In order to create the physical facilities locations in each area significant disruption will occur, both in construction and in movement of network elements / equipment.
- Building appropriate physical facilities can be costly, with no direct payback visible, and as such may come under closer scrutiny from external stakeholders.

4.0 Strategy/Approach

Review photographs taken during site visits to classify the IS&T room requirements for each location, apply knowledge of Hydro's technology strategy and determine the equipment needed to meet standards.

Hydro Place

Hydro Place was addressed in the design brief referenced above and the following IS&T rooms were identified:

- Core Telecommunication Room located on level two in the Network Center.
- Core Server Room located on level one in the computer room.
- Seven Class two Telecommunications Rooms; one on each of the six floors and one additional room on level two.

1. The Core Telecommunications Room and the Core Server Room meet the standards and no additional equipment is required. Hydro must continue to ensure that any equipment added to these locations is connected directly to the batteries or sufficient UPS is supplied to provide power till the generators kick in.

2. The seven Class 2 IS&T Rooms require 200VA UPS to maintain power to the switches until the generator kicks in. The rooms are located in the center of the building surrounded by air-conditioned walls so temperature should not be a problem.

Bishops Falls

Bishops Falls was addressed in the design brief referenced above and the following IS&T rooms were identified:

1. The main room in Bishop's Falls will be designed as a Class 1 IS&T Room. It shall consist of four racks:

   - Server Rack
   - UPS Rack
   - LAN Switching Rack (already existing)
   - WAN communication Rack (already existing)

   This room will need and computer rack and a miscellaneous rack, temperature should not be an issue because the room is air-conditioned. The servers and UPS's a in this location are currently placed on a shelving unit and must be moved to the racks.

Due to the size and position of the warehouse and salvage stores offices it is necessary to install two Class 4 IS&T Room facilities in the far two corners of the building with respect to the main IS&T Room One of these Class 4 IS&T Room facilities will service the Material Management area and the other Class 4 IS&T Room will service Salvage Stores offices and the RCM building.

2. Material Management Class 4 IS&T room.
   This location requires a wall mounted rack and UPS and the existing equipment must be re-located to the rack. Temperature should not be an issue because there will only be one switch and the UPS in the cabinet.

3. Salvage Stores Class 4 IS&T room.
   This location requires a wall mounted rack and UPS and the existing equipment must be re-located to the rack. Temperature should not be an issue because there will only be one switch and the UPS in the cabinet.

As for outlying buildings on the Bishop's Falls site, the following facilities will be established:

4. The maintenance building will have a Class 2 IS&T Room.
   A switch rack and UPS is required for this room and the equipment must be relocated to the rack.

5. The diesel building will have a Class 3 IS&T Room.
   A switch rack and UPS is required for this room and the equipment must be relocated to the rack. A rack mounted air-conditioning unit will also be installed.

6. The security building will have a Class 3 IS&T Room. A rack mounted air-conditioning unit will be installed. A switch rack and UPS is required for this room and the equipment must be relocated

to the rack. A rack mounted air-conditioning unit will also be installed.

Holyrood

Holyrood was addressed in the design brief referenced above and the following IS&T rooms were identified:

1. The main IS&T room in Holyrood Plant will be designed as a Class 1 IS&T Room It shall consist of three racks

   - WAN Server Rack
   - UPS Rack
   - LAN Switching Rack

   This room needs a new server rack and a switching rack, we can re-use one of the existing racks as a miscellaneous rack for the UPS and other items. A UPS is needed for the switching rack with a capacity of 850 VA or better. There is air conditioning in this room so temperature should not be an issue.

Because of the size and layout of the building, it is impossible to service all LAN devices from the main IS&T room therefore two additional rooms are required as follows:

2. A separate room defined as a Class 2 IS&T services all LAN devices in the office area. This room has a rack so a UPS rated at 500 VA or better will bring it up to code. This room has the potential for temperature problems so a rack mounted air conditioner is recommended.

3. A Class 4 IS&T Room services a number of LAN devices in the Electrical Shop area. This area will require a wall mounted enclosure and UPS rated at 200VA. Temperature should not be an issue because of the low device count.

Churchill Falls

Churchill Falls and the remaining sites were not addressed in the design brief so xwave will classify the requirements for these sites and detail the equipment needed to bring them up to specifications. This location is the second and last site within the Hydro to utilize a separate Core Telecommunications Room and Core Server Room. This location has several outlying building and three remote locations connected via a MAN (Metropolitan Area Network).

1. The Core Telecommunications Room is located on the lower level of C&A building. This location has fire suppression and a separate air conditioning system and requires a switching rack to bring it up to code.

2. The Core Server Room is located on the second floor of the C&A building. This room needs a non-water based fire suppression system, separate air conditioning, a server rack, a miscellaneous rack and two UPS rated at 2000VA and 850VA.

3. The plant has one network termination point and a Class 4 IS&T enclosure and a 200VA UPS will bring it up to code. Heat should not be a problem because of the low device count and location.

4. The Fire and Safety building has one network termination point and can be serviced by a single Class 4 IS&T enclosure and a 200VA UPS. Heat should not be problem here because of the low device count.

5. The networking equipment for the warehouse is terminated on a rack in a secure room and a 850VA UPS is all that is required create a Class 3 IS&T Room. Heat should not be a problem at this location because of the low device count and location of the room.

6. The Town Offices main building has a fiber connection to the Town Services building and the school. There is a file and print server on the main floor of this building which should be re-located to a server rack in the basement. The networking gear is in a locked room in the basement and can become a Class 1 IS&T room by adding a server rack and miscellaneous rack. UPS rated at 2000 VA and 850 VA is required as well.

7. The Town Services building has one network termination point and is enclosed in a locked wall mounted cabinet, the only item needed to create a Class 4 IS&T Room is a 200VA UPS.

8. The school network is not connected to the corporate network and all server and networking devices are mounted in the same rack. This area could be converted to a Class 3 IS&T cabinet if the existing open rack was replaced by an enclosed rack and an additional 850VA UPS was installed.

9. The airport Services building houses a file and print server and one network termination point. This building is best serviced by creating a Class 3 IS&T rack. A fully enclosed rack and 850VA UPS is

required to accomplish this. The server must be moved from the shelving unit to the rack.

Bay D’espoir

This location has a main building which houses a pair of servers and one network termination point, and several outlying building. The main building has the networking equipment and the servers located in separate rooms.

1. The main building communications room needs a 850VA UPS to bring it up to code.

2. The servers at this location are placed on a shelving unit located in a common area within the office section. A Class 3 IS&T enclosed cabinet is required at this location to meet standards.

3. The garage building is connected to the office building via fiber and all networking equipment is contained within a wall mounted enclosure. A 200VA UPS is required at this location to create a Class 4 IS&T Room.

4. The Telecontrol building is connected to the office building via fiber and all networking equipment is contained within a wall mounted enclosure. A 200VA UPS is required at this location to create a Class 4 IS&T Room.

5. The Line Depot building is connected to the office building via fiber and all networking equipment is contained within a wall mounted enclosure. A 200VA UPS is required at this location to create a Class 4 IS&T Room.

6. The Security building is connected to the office building via fiber and all networking equipment is contained within a wall mounted enclosure. A 200VA UPS is required at this location to create a Class 4 IS&T Room.

7. The Warehouse building is connected to the office building via fiber and all networking equipment is contained within a wall mounted enclosure. A 200VA UPS is required at this location to create a Class 4 IS&T Room.

Whitbourne

This location houses a combination file, print and Notes server and a single network termination. All the server and communication equipment is installed in one locked room.

1. The room can become a Class 3 IS&T Room by re-arranging the equipment in the existing rack, adding one 840VA UPS, a couple rack shelves and keyboard tray. The server must be moved from the table to the rack. Heating at his location may be an issue so a rack mount air-conditioner is required.

Deer Lake

This location does not house a server and has all networking devices located in one room.

1. A Class 2 IS&T Room can be created by adding a 500VA UPS to the existing rack. A rack mounted air conditioning unit is required to combat heat related problems.

Stephenville

This location houses a combination file, print and Notes server and one network termination point. All devices are located in a common locked room.

1. This room can become a Class 1 IS&T Room with the addition of a server rack, a miscellaneous rack and a UPS rated at 850VA. Heating at his location may be an issue so a rack mount air-conditioner is required. The server must be re-located to the server rack.

Port Saunders

This location houses a file server and one network termination point. All devices are located in a common locked room.

1. This room can become a Class 1 IS&T Room with the addition of a server rack, a miscellaneous rack and a UPS rated at 850VA. Heating at his location may be an issue so a rack mount air-conditioner is required. The server must be re-located to the server rack.

St. Anthony

This location has two buildings connected via leased line services, the main office houses a file server and one network termination point and the warehouse has one network termination point.

1. The main building has the server installed on a shelving unit and the networking devices mounted on an open rack in one un-locked room. This location is best served by replacing the open rack with a Class 3 IS&T enclosed cabinet. Two 850VA UPS and a rack mounted air-conditioner will bring this location up to specifications.

2. The warehouse has one network termination point which is enclosed in a wall mounted locked cabinet. The cabinet has a brick style UPS sitting in the rack which should be replaced with a rack mount 200 VAUPS.

Wabush

This location has a main building which houses a server and network termination point and a warehouse connected via leased line. The main building has the servers and networking devices located on a shelving unit in the hall. The warehouse has all equipment mounted in an enclosed rack.

1. The main building needs to re-locate all server and networking equipment to a fully enclosed Class 3 IS&T rack complete with dual 850VA UPS and rack mounted air conditioning unit.

2. The warehouse location has the equipment in an enclosed rack and the only item needed to update it to a Class 4 IS&T room is a 200VA UPS.

Goose Bay

This location has a main building with a server and network termination point and a warehouse connected via a wireless link. The main building has the server and networking equipment mounted in open racks in a common area. The warehouse has one network termination point.

1. The main building is the termination point for several leased line connections thus the communications rack is full so xwave recommends two Class 3 IS&T enclosed cabinets. The server equipment should be mounted in one cabinet and the communications equipment mounted in the other. Both cabinets require rack mounted air-conditioning and the communications cabinet needs and addition 850VA UPS.

2. The warehouse needs a Class 4 enclosed cabinet and 200VA UPS to bring it up to code.